Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JAN 2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**
4. TITLE AND SUBTITLE **CrossTalk: The Journal of Defense Software Engineering. Volume 20, Number 1, January 2007**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **OO-ALC/MASE,6022 Fir Ave,Hill AFB,UT,84056-5820**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**32**	

Departments

ON THE COVER

Cover Design by Kent Bingham

Additional art services provided by Janna Jensen

Unit Compliance Inspection: What Did We Learn?

In August 2006, the 402d Software Maintenance Group became a full-fledged member of the depot maintenance fraternity by subjecting itself to a Unit Compliance Inspection based on the same checklists as the aircraft, electronics, and commodities groups.

In effect, we were breaking new ground – we had always relied on the robustness of our Level 5 CMMI processes as a reason to be exempt from the standard Air Force maintenance instructions and checklists that our compatriots used. For our core business area (development and maintenance of operational flight programs and automatic test equipment software) that was definitely the case. Our work is centered on processes, not tasks. Our software engineers do not use work control documents nor do our technicians require special skills qualification.

So what do we have in common, and why did we examine our compliance with policy and procedures that were developed for a hardware maintenance environment? The answer is simple: We use tools, equipment, material, and technical data just like everyone else.

Air Force policy on tools is designed to both prevent foreign object damage and to reduce long term costs with better inventory control. Our software integration laboratories use equipment that requires periodic maintenance, calibration, and clear accountability. Material, whether bench stock, shop stock, or floating spares, is better managed when it is sorted, labeled, and regularly inventoried. Finally, technical data can never be accurate if it is not kept current and labeled appropriately.

How much effort was involved in becoming compliant? Tons! We sorted, scrubbed, straightened, labeled, shredded, recycled, shadowed, capped, taped, stamped, inventoried, and signed everything in sight. We inspected our labs from wall to wall with an eye out for safety hazards, excess material, stray tools, equipment overdue for calibrations, and general clutter.

Was it worth it? In the end, yes! While I doubt we'll see much direct benefit from the dozens of appointment letters I signed, the rest of our preparation has made an impact. Our labs are clean and free of clutter. Material, tools, technical data, and equipment are organized and accessible. Eliminating excess cabinets has freed up valuable floor space. Finally, we demonstrated that our CMMI Level 5 processes are compatible with – even complementary to – Air Force maintenance instructions. You can have quality processes and still be compliant.

Diane E. Suchan

Diane E. Suchan
Warner Robins Air Logistics Center Co-Sponsor

Choose Your Favorite

The purpose of this theme was to allow CROSSTALK to share articles on topics and from authors of special interest to us and I hope to you as well. Mike McNair was kind enough to write an article on some of the key issues to consider when merging hardware and software in *Where Hardware and Software Meet: The Basics*. Our next article by LTC Nanette Patton and Allan Shechet highlights some of the real obstacles that must be overcome when implementing process improvements such as Earned Value Management in *Earned Value Management: Are Expectations Too High?* I think many readers will have a curiosity for Duy Le, Dr. Rayford B. Vaughn, and Dr. Yoginder S. Dandass' article *Developments and Challenges of Internet Development in Vietnam – A General Perspective*. COL Kenneth L. Alford and Steven R. Ditmeyer also consider net-centric concerns in *Net-Centric Operations: Defense and Transportation Synergy*. Finally, as more and more organizations climb the software maturity ladder, I believe it is reasonable to ask, *What's next?* Donald J. Reifer proposes his suggestion in *Profiles of Level 5 CMMI Organizations*.

Elizabeth Starrett

Elizabeth Starrett
Publisher

Announcing CrossTalk's Co-Sponsor Team for 2007

Elizabeth Starrett
CrossTalk

It is with great appreciation that I announce CrossTalk's co-sponsors for 2007. The support from these leaders in the software community makes it possible to provide CrossTalk at no cost to software professionals. This year, the returning co-sponsors, including the Naval Air Systems Command, the three U.S. Air Force Air Logistics Centers' Software Maintenance Groups, and the U.S. Department of Homeland Security welcome the Assistant Secretary of Defense (Networks and Information Integration) – Department of Defense Chief Information Office. Please look for their contributions each month in our From the Sponsor column found on page 3. Their organizations will also be high-lighted on the back cover of each CrossTalk.

The Honorable John Grimes, Department of Defense – Chief Information Officer

The ASD(NII)/DoD-CIO is the principal staff assistant and advisor to the Secretary on networks and network-centric policies and concepts, command and control, communications, non-intelligence space matters, enterprise-wide integration of DoD information matters, and Information Technology. Additionally, the DoD-CIO has responsibilities for integrating information and related activities and services across the DoD. The mission of the organization is to *enable Net-Centric operations*. NII/CIO is leading the Information Age transformation that will enhance the DoD's efficiency and effectiveness by establishing an *Information on Demand* capability. See <www.dod.mil/cio-nii/> for more information.

Terry Clark, NAVAIR, Systems Engineering Department – Director, Software Engineering

The Naval Air Systems Command (NAVAIR) provides the cost-wise readiness and dominant maritime combat power to make a great Navy/Marine Corps team better. The NAVAIR team, in partnership with industry, is committed to serving the nation by balancing current and future readiness while developing, acquiring, and supporting naval aeronautical and related technology systems with which the operating forces, in support of the unified commanders and our allies, can train, fight, and win. See <www.navair.navy.mil> for more information.

Kevin Stamey, 76 SMXG Director

The 76th Software Maintenance Group at the Oklahoma City-Air Logistics Center is a leader in the avionics software industry that understands total system integration. The center has a proven record of producing software on time, on budget, and defect-free. Its people provide the expertise, software, weapons, interface, and aircraft systems that are fully integrated to ensure dependable war-winning capabilities. Its areas of expertise include navigation, radar, weapons and system integration, systems engineering, operational flight software, automatic test equipment, and more. See <www.bringittotinker.com> for more information.

Randy Hill, 309 SMXG Director

The 309th Software Maintenance Group at the Ogden-Air Logistics Center is a recognized world leader in cradle-to-grave systems support, encompassing hardware engineering, software engineering, systems engineering, data management, consulting, and much more. The division is a Software Engineering Institute Software Capability Maturity Model® (CMM®) Integration Level 5 Organization with Team Software Process℠ engineers. Their accreditations also include AS9100 and ISO 9000. See <www.mas.hill.af.mil> for more information.

Diane Suchan, 402 SMXG Director

The 402d Software Maintenance Group at the Warner Robins-Air Logistics Center provides combat-ready weapon systems, equipment, services, and support personnel for the U.S. Air Force. The center is a leader in systems engineering, safety engineering, human factors engineering, advanced design and manufacturing engineering, and logistics engineering support. The center has responsibility for the sustainment of the F-15 Eagle, C-130 Hercules, C-141 Starlifter, C-5 cargo aircraft, U-2 surveillance aircraft, all Air Force missiles, all Air Force helicopters, and more. See <https://www.mil.robins.af.mil> for more information.

Joe Jarzombek, Department of Homeland Security – Director of Software Assurance

The Department of Homeland Security (DHS) National Cyber Security Division serves as a focal point for software assurance, as part of ensuring the security of cyberspace, and works closely with the private sector, academia, other government agencies, and international allies to improve software development and acquisition processes that will lead to better quality and more secure software. DHS provides the public-private framework for shifting the paradigm from patch management to software assurance. See <www.us-cert.gov> and <https://buildsecurityin.us-cert. gov/portal> for more information.

CrossTalk still has one 2007 issue in need of sponsorship support. For more information about joining our government leaders, please contact Elizabeth Starrett at (801) 775-4158 or <beth.starrett@hill.af.mil>.

®   Capability Maturity Model and CMM are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

℠   CMM Integration and Team Software Process are service marks of Carnegie Mellon University.

The 2007 CROSSTALK Editorial Board

Elizabeth Starrett
CROSSTALK

CROSSTALK proudly presents the 2007 CROSSTALK Editorial Board. Each article submitted to CROSSTALK is reviewed by two technical reviewers from the list below in addition to me, CROSSTALK'S publisher. The insights from the board improve the readability and usefulness of the articles that are published in CROSSTALK. Most reviewers listed have graciously offered their own time to support CROSSTALK's technical review process. We give very special thanks to all those participating in our 2007 CROSSTALK Editorial Board.

Where Hardware and Software Meet: The Basics

Mike McNair
Science Applications International Corporation

Effective integration of hardware and software requires an understanding of fundamental concepts such as a bit, address, and interrupt. Using these concepts in the context of protocols and applications is what makes an interface useful. This article looks at these fundamental concepts from a software view and then applies them to simple applications where they can be used to expand into other application domains and uses of hardware and software.

From a software perspective, it is important to understand two differing models: one that reflects a software engineer's representation of a system in software, and the devices and processes of the actual system. At its core, software is a model represented in terms of data structures and algorithms. Ideally, these constructs parallel something physical and do so with a high degree of accuracy. The reality is that software not only models a physical construct but also contains its own information (a *meta construct* of sorts) to help manage that physical model. In a simple example, a byte array may represent a message, but in the software model there may be bookkeeping to track the length of the array or a pointer to the body of the message contained within the array. These features are used to help manage manipulation of the byte array but are not a part of the actual stream of bytes as transferred over an interface.

Understanding the interplay between hardware and software requires an understanding of not only the hardware but the model used to represent it. This software model attempts to represent the actual hardware as closely as possible. For the software, the hardware model is represented by target or memory maps, interrupt handlers, addressing schemes,

board support packages (BSPs), and other constructs. Throughout this article, these will be discussed in a context that hopefully pulls together a generic view of a hardware model from a software perspective. It is by understanding this view that we understand how hardware and software work together at their lowest levels.

Basic Concepts

There are some basic hardware features that are simple yet commonly misunderstood by software engineers. If a software developer can grasp the fundamental characteristics of bits, interrupts, and addresses, they will have the building blocks needed to understand how hardware and software interface with each other. The following discussion is generic due to the wide range of hardware that is available, but explains concepts based on common features and approaches to current hardware.

Basic Concept: What Is a Bit?

To a software developer, a bit is a value – usually thought of as 1 or 0 and abstracted as on/off, true/false, or other paradigms. In hardware, a bit is not only a voltage level but is a voltage at a certain time. In the hardware, a value of 1 is assigned a certain voltage, and 0 is assigned another voltage. As the voltage levels change, there is a timing clock that tells the hardware when to sample the signal. Depending on the sensed voltage, the hardware identifies the signal as being either in a 1 state or a 0 state.

Graphically, consider the following for the bit pattern of the letter V (decimal ASCII code 86). In binary, this would be represented as 01010110. This string of bits can be depicted from both a software and hardware view as shown in Figure 1.

In order to transition from the software model to the physical model of actual voltages, the hardware has timing circuitry that *cuts* the voltage stream into bits and identifies those bits. By putting all three forms together, their relation

becomes a little clearer.

With this more integrated view, there are other concepts that begin to come into play. For example, the concept of *data rate* is not just how many bits can be transferred per second, but how fast the timing circuit can create pulses so the hardware is able to sense voltage levels and, therefore, discretely identify bits as shown in Figure 2. Grasping the concept of a bit really is the key to understanding most interfacing concepts and issues.

Basic Concept: What Is an Address?

An address, simply put, is the location of something. From a software perspective, addresses represent the placement of various things: executable code, interfaces, interrupt handlers, data, etc. While software typically treats an address as a means of labeling, hardware uses addresses to actually locate things – whether it is where a wire connects to a processor, where data is stored in memory, etc.

In many applications, actual addresses are *hidden* through the use of identifiers in source code, virtual addressing, and other schemes; the point being that most application software is not truly concerned with the real address but just requires access to the address. The closer the implementation gets to the hardware, however, the more important it is to know where things are stored and to represent that location with the actual physical address. It is at this level that artifacts like memory maps and BSPs become extremely useful.

Digressing for a moment, a memory map can be thought of as an allocation of memory regions. Throughout the possible range of physical addresses, certain uses of the memory can be assigned to one region or another. The operating system (OS) and application are either constrained or assumed to honor these allocations. A BSP is a special extension of a memory map as it includes not only an identification of the memory regions, but

Figure 1: *String of Bits for Letter V*

Software View

0 1 0 1 0 1 1 0
Bit Pattern for the Letter V

Hardware View

0 1 0 1 0 1 1 0
Conceptual Voltage Levels
for the Letter V
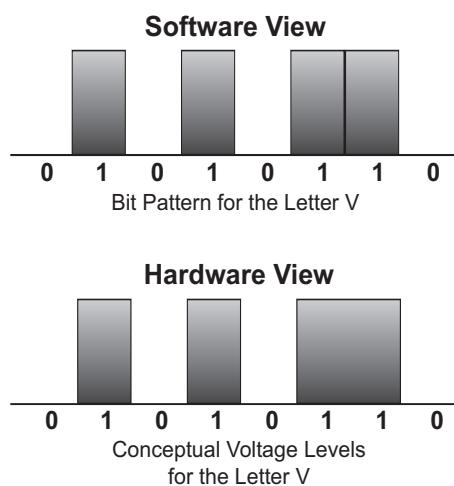
static data and code used by the underlying OS to manage the application. Things like maximum stack size for function calls or device addresses can be found in a BSP.

Simplistically, memory is conceptually divided into volatile and non-volatile memory. Volatile memory (e.g., random access memory) loses its contents when there is no power while non-volatile memory (disk drives, memory sticks, etc.) has a means of preserving its contents across power cycles. Of course, there are various forms of each kind of memory. When these are all interconnected in a computer system, the overall range of addresses (physical address space) grows.

From a software view, memory has to be looked at as not just the type of memory (with its associated capabilities and constraints), but also how that memory is used. The OS usually manages memory for high-level applications, but at a low level it is important to understand memory type and memory use. In essence, memory management is a manipulation of statically allocated and dynamically allocated memory regions (see Figure 3). Statically allocated memory regions usually contain things like object code, interrupt mapping tables, static data, etc. Dynamically allocated memory regions include data areas created during run time – things like dynamically sized queues, linked lists, and other similar constructs.

When a hardware device is accessed, commands are sent to a specific address associated with that device. The addresses available for this are usually reserved and protected from other uses by segmenting the memory into regions as shown in Figure 3. Physically small microprocessors can have as few as 10-15 pins; more capable, general-purpose processors can have more than 100 pins. Some of these pins are designated as data lines and address lines. In the actual circuitry these lines are physically connected to memory devices, system buses, device controllers, and other system components. It is through these connections and the ability to specify addresses of specific locations that devices can be controlled and monitored.

Most things that can be manipulated by software have an address. Of course, a specific piece of data has an address in memory. Likewise, hardware interfaces are known by the address of their control and data lines. The processor can be manipulated by knowing the address of its registers. Interrupt handlers must be placed at specific addresses. Think of knowing an address as the key to controlling and using a device or function in the computer system.
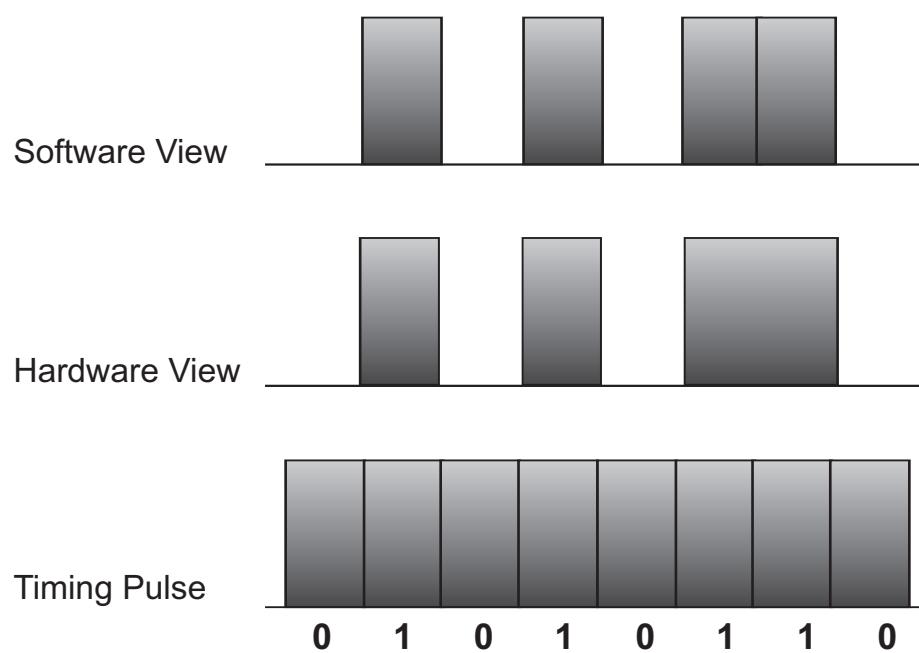
Figure 2: *Software and Hardware Views for the Letter V*

Basic Concept: What Is an Interrupt?

Some interfaces do not transfer data but instead are designed to transfer control signals. Even in a simple RS-232 serial interface, there is more on the cable than just a stream of bits. Some of the individual wires carry control signals. In the hardware, these signals are designated with voltages – just as with bits. The change in voltage on these control wires (transitions) act to signal an event. In order for the hardware to notify the processor that a transition has occurred, it generates what is known as an interrupt. As long as the sensed voltage does not cross whatever the voltage threshold is, there will not be an interrupt.

Using Figure 4 (see page 8) as a reference, consider what happens during the handling of an interrupt. Within the processor, an interrupt is generated when the hardware senses a voltage transition – usually through a control line (1 in Figure 4). When this control signal is sent to the processor, the processor generally interrupts some or all of its processing (depending on the priority of the inter-

Figure 3: *Memory Regions*
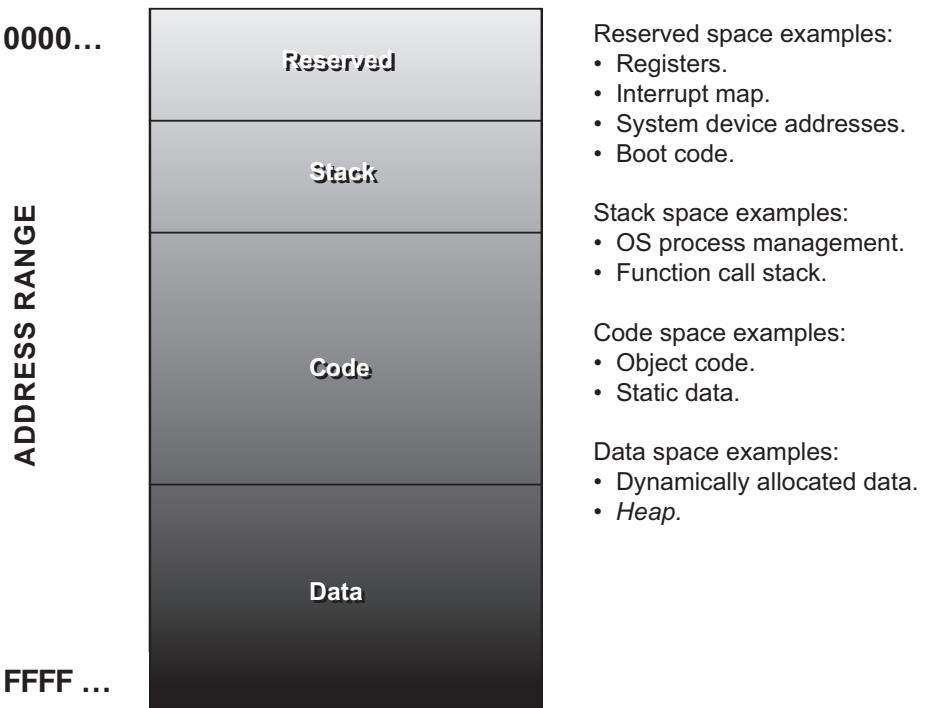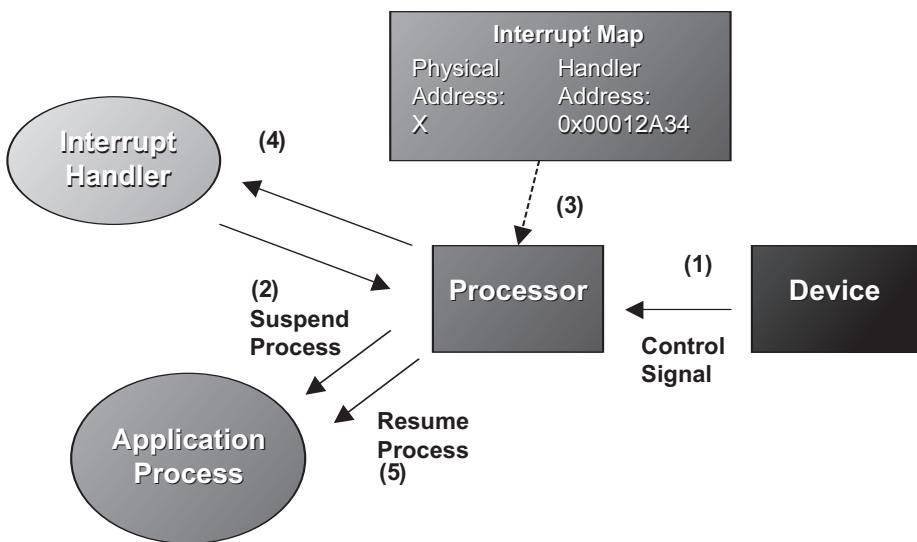
Figure 4: *Handling of an Interrupt*

rupt) in order to do something with that signal (2 in Figure 4). Most OS allow for the concept of an interrupt handler. Since this signal enters the processor at a particular physical address, there must be a means of mapping the physical address of the control signal to the address of an interrupt handler (3 in Figure 4). The OS then handles passing control from whatever code is currently being executed to the interrupt handler by using a table lookup that cross references the physical address of the signal to the start address of the interrupt handler code (4 in Figure 4). When the interrupt handler has completed its execution, the OS resumes execution of the interrupted code (5 in Figure 4).

Because interrupt handlers truly interrupt what a processor is doing, they are usually written to be executed quickly. Generally, an approach of temporarily storing data or state and then exiting is common. The longer an interrupt handler takes to complete, the less time there is for other processing within the computer. At an application level, this can have a tremendous impact on any time critical processing. At a low level, it is possible to have interrupts arrive at a high-enough rate that if a handler takes too long, the next interrupt will not be handled. Should this happen, an event is missed – possibly with corresponding data. In a mission-critical system, either changing critical processing timelines or missing an interrupt can be disastrous.

Putting It All Together
Many real-world systems rely on software

controlling some hardware device through an address or interrupt. With the advancement of technology, many variations exist on these themes, but once these basic concepts are understood, it is relatively simple to expand the concept into the new implementation.

As a way of bringing the simple concepts in this article together, briefly consider two examples: turning on a light emitting diode (LED) and turning on a motor. While these may seem uninteresting, it is important to realize that an LED can indicate whether power is applied to a device, a weapon system is ready to fire, or a strobe light effect can be achieved by simply turning the LED on and off. Likewise a motor can be used to control the spin of media in a CD player, the speed of a wheeled vehicle, or the arm of a robotic device.

Example: LED Control
An LED is a simple device that only needs power applied to it to turn it on and power removed from it to turn it off. Since a bit is actually mapped to a voltage, a very simple implementation for controlling an LED would be to wire the electrical interface to a specific address or port on the processor where the controlling code is executing. By writing a 1 to that port, the LED can be turned on; by writing a 0 to that port, the LED can be turned off. The port in this case can be either an actual address or processor register. Either way, the operations are simply achieved by writing a value to a specific location. By including a delay between the ON and OFF writes and placing the code in a loop, it is possible to *blink* the LED at a desired rate.

Example: Simple Motor Control
For software to control a motor, there almost always needs to be a hardware controller that provides a somewhat intelligent interface between the processor executing the software and the motor itself. As a result, the application does not talk directly to the motor but instead talks through a controller. Consider a simple model of a motor that has these operations: set motor speed, set motor direction, get motor speed, and get motor direction. The controller provides the interface for actual control of the motor in response to these simple commands. As with an LED, the controller allows command messages to be written to a specific address and return data (due to the *get* commands) be sent at another address.

From within the application, the command to set the direction of the motor

Figure 5: *Retrieving a Current Value*

Message Set		
Name	**ID**	**Data**
Set Direction	01	0 = clockwise spin
		1 = counter-clockwise spin
Get Direction	02	no data
Current Direction	03	same as Set Direction
Set Speed	04	0 = stop
		1.255 = values for speed
Get Speed	05	no data
Current Speed	06	same a Set Speed

  * A message for this motor would be composed of a byte for Message ID and a byte for Message Data.

spin is achieved by sending the correct command message to indicate direction. Likewise, motor speed is achieved by sending a command message with a quantification of speed (maybe 1.255 for a byte data field where 0 = stop). Retrieving the current value of either of these is achieved by sending the proper command message and reading for the returned value from the controller – each usually at two different addresses as shown in Figure 5.

Given these operations, an accelerator pedal on an electric car, for example, can be used conceptually like a joystick to supply speed values to the motor. The controlling software merely reads the amount of pedal depression and converts it to a value that is appropriate for the motor controller. (Changing the vehicle direction from forward to reverse could be a button that the software reads the state of and then sends an appropriate motor command to the motor controller.) For the operator of this vehicle, a separate task can periodically read the value for motor direction and motor speed, scale the speed as needed to map it into the appropriate units (km/hr), and display the result to an operator.

Making It Happen

A key piece to implementing low-level interfaces is the support provided by the processor, OS, and development environment. Processors will vary in terms of address width (8 bit, 16 bit, 32 bit, etc), addressable memory range, number of registers, and number of interrupt lines (etc.), where these are in addition to characteristics like processor speed, cache size, and physical memory. Each of these characteristics must be matched up to overall system performance, number and type of external devices, and other considerations.

In Conclusion: Expanding the Applications

In order to facilitate the management of low-level interfaces to devices, a set of code is written to encapsulate and handle the nuances of the interface and device. This abstraction is referred to as a device driver. To its applications, a device driver presents a set of operations to control and manage the device, but many times actually communicates with the controller of the device and not the device itself. At its lowest levels, a device driver handles the intricacies of handling interrupts, formatting and parsing command messages, providing sequencing as

required, and performing other device specific activities. A device driver is simply a device or interface manager that is built on the manipulation of bits, addresses, and interrupts.

The simple concepts of bit, address, and interrupt cover most types of hardware/software interfaces at a low level. Overlaid on these low-level constructs are various protocols (message and communication protocols, Universal Serial Bus, and other device and application specification paradigms) to control more sophisticated coordination on both sides of the interface. Even though the addition of protocols presents complication to the implementation of the interface, the interface itself is fundamentally represented in terms of control (signals and interrupts) and data (streams of bits and addresses).◆

Additional Reading

1. Embedded.com <www.embedded.com>.
2. Programmer's Heaven <www.programmersheaven.com/zone7/index.htm>.
3. Device Software Optimization <https://dso.com>.
4. Heath, Steve. Embedded Systems Design. 2nd edition. Newness, June 2002.

About the Author

Mike McNair is a senior systems engineer for Science Applications International Corporation where he is a part of the chief engineer team for unmanned ground vehicles on contract to the U.S. Army. His background includes more than 20 years of experience as a programmer, technical lead, and software program manager on projects ranging in size, complexity, and target for a variety of customers. He has also served on several process improvement (including Software Engineering Process Group lead) and training initiatives.

Science Applications International Corporation
8303 N Mopac
STE B-450
Austin, TX 78759
Phone: (512) 366-7834
Fax: (512) 366-7860
E-mail: michael.k.mcnair@saic.com

Earned Value Management: Are Expectations Too High?

LTC Nanette Patton

Office of the Surgeon General

Allan Shechet

Savvy Services Inc.

Earned Value Management Systems (EVMS) are frequently required on government Automated Information System programs. When implementing EVM, especially for the first time, agencies should train their key managers not only in the EVM process but also in the behaviors and management styles required to avoid major problems that can result from the implementation. While EVM is a useful project management tool, implementing EVM will not solve all the challenges in achieving project goals. Furthermore, given the funding and selection processes for programs, first time EVM implementation can introduce a whole new set of program management challenges. Based on their experience with information technology (IT) and aerospace projects, the authors identify potential difficulties and risk mitigation strategies to counter those potential difficulties.

The President's Office of Management and Budget (OMB) has asked federal agencies to use a project management discipline known as EVM as a strategy to avoid costly IT failures. Other than within the Department of Defense (DoD), EVM is not well understood by federal agencies [1]. OMB issued its EVM policy guidelines in two memos issued in August 2004 and August 2005. In addition to requiring federal agencies and their contractors to use EVM for managing all major IT projects, the OMB established new reporting requirements. Agencies must include EVM data when they submit Exhibit 300s, documents in which they present their business cases for major IT projects. The OMB requires agencies to use EVM to calculate and report each project's estimated total cost and completion date.

While EVM is an effective and useful project management tool, there are constraints within the organizational environment of the federal government that impede a smooth implementation of EVM.

Federal Chief Information Officer (CIO) Council Framework

In December 2005, the federal CIO Council released "A Framework for Developing EVMS Policy for IT Projects" [2] to assist agencies in developing their EVM policies as required by OMB Memorandum M-05-23 [3] for major IT projects. The guidance states the following:

> EVM is a project management control tool allowing visibility into technical, cost and schedule planning, performance, and progress for major IT projects. EVM not only encourages contractors to use effective internal cost and schedule management control systems, but also provides the manager with timely and consistent cost, schedule, and progress data. The implementation of an EVMS ensures that cost, schedule, and technical aspects of the contract are truly integrated and estimated, and actual progress of the project can be identified. [4]

> **"If the budget spend plan shows the project over-spending and the project schedule ... slipping, the PM ... may have no way to make a quantitative assessment of how bad the trouble is."**

EVM Basics

Program managers (PMs) should manage project cost and schedule performance measurements as integrated elements and not as separate entities. If the budget spend plan shows the project over-spending and the project schedule shows milestones slipping, the PM may know they might be in trouble but may have no way to make a quantitative assessment of how bad the trouble is. EVMS solves this problem by providing an accurate picture of spending and accomplishments related to a baseline plan. This enables the PM to quickly form conclusions about the project team's staffing levels and productivity, as well as giving insight into areas of the work breakdown structure where the problems occur.

EVM compares the following three pieces of information:
1. How much work you planned to have accomplished until now (in dollars or hours) is called the *Planned Value* (PV).
2. How much you have actually spent until now (in dollars or hours) is called *Actual Cost* (AC).
3. The value, in terms of your baseline budget, of the work accomplished until now (in dollars or hours) is called the *Earned Value* (EV).

The first two pieces of data are compared to the EV in terms of differences resulting in variances and ratios resulting in performance indexes.

Basic EVM calculations involve differences or ratios with respect to EV:
1. The difference between EV and your plan (PV) is Schedule Variance (SV). $SV = EV - PV$.
2. The difference between EV and your spending (AC) is Cost Variance (CV). $CV = EV - AC$.
3. The ratio of EV to plan (PV) is your Schedule Performance Index (SPI). $SPI = EV/PV$.
4. The ratio of EV to cost (AC) is your Cost Performance Index (CPI). $CPI = EV/AC$.

Positive variance is favorable and negative is unfavorable. Having an EVM performance index that is greater than 1 is favorable, and less than 1 is unfavorable.

CPI is a reading on productivity and SPI is a reading on progress. If there is good productivity and slow progress, then the project is understaffed. If there is low productivity, then either the project has too much unplanned work or the project manager may have estimated poorly and the project has more work content than

previously thought.

That is the essence of EVM; the rest are details.

DoD EVM Applicability

The DoD has been using cost and schedule controls on aerospace and defense projects since the mid-60s. In the Office of the Under Secretary of Defense (Acquisition Technology and Logistics) policy memorandum dated March 7, 2005, the DoD revised its EVM policy *to streamline, improve, and increase consistency in EVM implementation and application* [5]. The DoD requirement for EVM applies to cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements that meet the dollar thresholds prescribed (see Table 1). This memorandum requires the Table's application thresholds (total contract value including planned options in then-year dollars [TY$]).

Although EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements valued at less than $20 million (total contract value including planned options) and/or less than 12 months in duration including options, PMs have the discretion to implement an EVMS. If implemented, the PM is required to conduct a cost-benefit analysis. The purpose of the cost-benefit analysis is to explain the rationale for the decision to require cost/schedule visibility in the contract and to substantiate that the benefits to the government outweigh the associated costs. If the value of a contract is expected to surpass $20 million or last longer than 12 months, acquisition guidelines suggest that the PM should consider imposing an EVM requirement on the contract.

The Defense Acquisition Guidebook discourages the application of EVM on firm-fixed price contracts, subcontracts, intra-government work agreements, and other agreements regardless of dollar value [6]. If knowledge by both parties requires access to cost/schedule data, the first action is to re-examine the contract type (e.g., fixed price incentive). However, in extraordinary cases where cost/schedule visibility is required and cannot be obtained using other means, the PM is required in accordance with acquisition guidelines to obtain a waiver for individual contracts from the Milestone Decision Authority (MDA)[1]. In these cases, the PM is required to conduct a business case analysis that includes rationale for why a cost or fixed price incentive contract was not the

Contract	Threshold	Requirements
Cost or Incentive Equal to or Above Threshold	≥ $50M	• Compliance with industry EVM standard. • Formal validation of contractor's EVM system. • Contract Performance Report. • Integrated Master Schedule. • Integrated Baseline Review. • Ongoing surveillance.
Cost or Incentive Less Than Upper Threshold but Equal to or Above Lower Threshold	< $50M but ≥ $20M	• Compliance with industry EVM standard. • Formal system validation not required. • Contract Performance Report (tailored). • Integrated Master Schedule (tailored). • Integrated Baseline Review (tailored). • Ongoing surveillance.
Cost or Incentive Less Than Threshold	< $20M	• EVM optional (risk-based decision). • Cost-benefit analysis required.

Table 1: *DoD EVM Thresholds and Requirements*

proper contracting vehicle. When appropriate, the business case analysis should be included in the acquisition approach section of the program acquisition strategy (see Figure 1).

However, the Federal Acquisition Regulation (FAR) council issued a rule in July 2006 that went into effect in August 2006 and gave federal agencies broad discretion in determining when and how to use EVM [7]. The council noted *that agencies have significant discretion in determining the size and complexity of projects that meet the criteria for a major acquisition set by the agency* [8]. While the council determined agencies could set their own dollar thresholds under this new rule, they also stated, *it is not appropriate to exclude certain contract types from EVMS requirements in the FAR. In accordance with OMB Circular A-11, Part 7, EVMS is required for major acquisitions for development regardless of contract type* [8]. The DoD allows exemptions. The Defense Federal Acquisition Regulations Supplement (DFARS) has its own proposed rule on EVM. That rule was published in January 2006 and was open for public comment until late March [9]. The DFARS proposed rule, which would be subordinate to the FAR rule, is now under review.

Figure 1: *Decision Process for EVM Application*
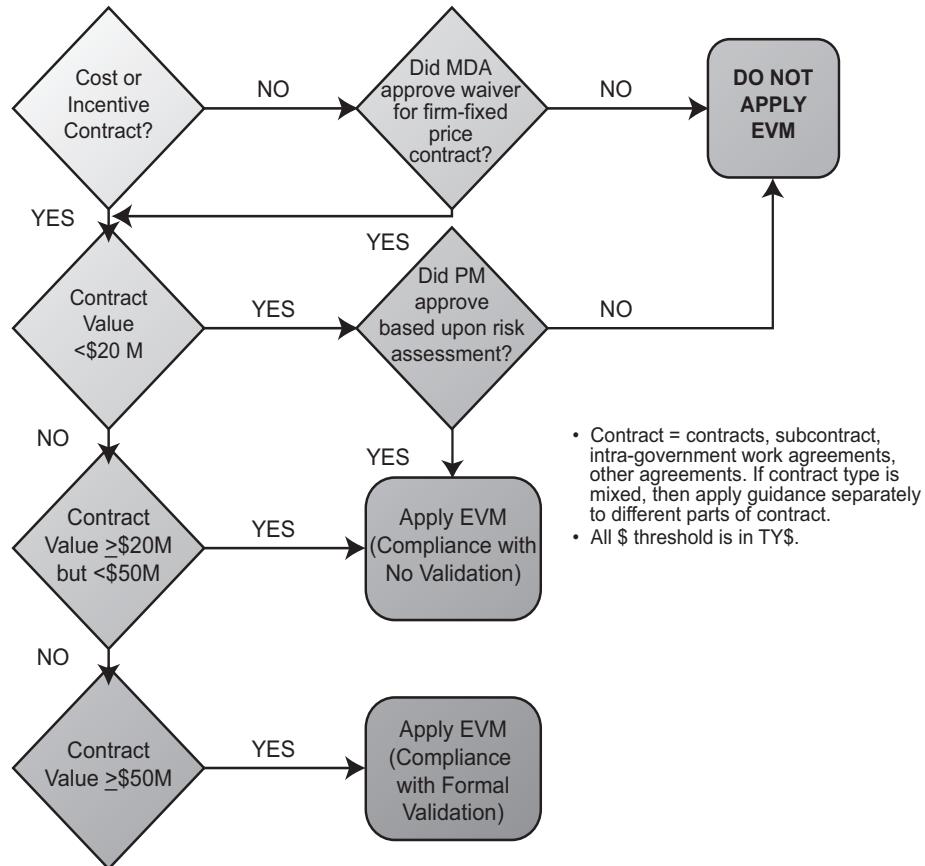
The Challenges of EVM in Practice

As federal agencies learn how to apply the principles of EVM to manage IT projects, they have encountered obstacles and challenges. Some of the challenges are related to the suitability of EVM itself to IT projects. Some of these challenges are cultural in nature as most experts say EVM cannot help agencies that cannot accept bad news. The experts say EVM is most valuable if agencies use it to help people learn from their mistakes rather than to punish them. Nevertheless, the fear of punishment must be addressed. Change management becomes a difficult aspect of bringing EVM into an agency in order to keep employees involved and ensure appropriate use of the EVM system. Some of the challenges are related to putting the infrastructure in place to support the EVMS process. It takes a lot of commitment and effort to get tools and systems in place and integrate them with other existing systems to generate the data and timely reports required.

Cultural/Perceptual Challenges

In theory, the EVMS enables PMs to track money spent on a project as well as measure the work accomplished against that cost and the schedule in a near real-time status. However, this theory does not always translate well in an actual project management setting. Speculations as to why EVMS may be ineffective include the following ideas:

- Lack of senior management support.
- Little understanding of EVM methodology as it pertains to software versus hardware and the accompanying belief that IT projects are not measurable and therefore EV cannot be applied to those projects [1].

- The need for employees trained in the concepts and methodologies.
- The perception that EVM is burdensome and somewhat costly to implement [10].
- The perceived questionable cost benefit of applying EVM to already budgeted IT projects [11].
- The perception that EVM measures the quantity but not the quality of work performed [1].
- EVMs underlying assumption that problems derive from poor project execution rather than inadequate project planning [1].

Depending on how deeply ingrained these perceptions are and the knowledge of the workforce on EVMS concepts, the PM will have to address these cultural issues.

Budget and Contracting Challenges

In applying EVM, having a realistic baseline is critical. However, in the federal arena, there are several systemic realities that can introduce errors to the baseline from the very beginning.

The process for creating the initial funding estimate can introduce errors. Developing a baseline budget is usually dependent on having experience with previous projects of similar type, size, and scope. In today's DoD IT environment in which we are trying to develop architectures with complementary infostructures[2] that support net-centric operations, we are venturing into uncharted territory in which we are pursuing project objectives that have not been achieved before in terms of technology, size, and scope. Furthermore, the initial budgetary funding estimate is usually based on well intentioned, but nevertheless *best guess* assumptions about how much change or rework is likely to occur as requirements

are clarified during the design phase and hence how much cost and schedule risk is associated with the new program. This budgetary estimate is then overly constrained years too early in the Planning, Programming, Budgeting, and Execution (PPBE) process to secure adequate funding. In the PPBE process, requirements are identified years before a budget is prepared and submitted. These requirements are expressed in the Future Year Defense Program. The planning cycle is shown in Table 2.

Given the rapidly changing environment of technology, the estimates are often too low. Because the budget is constrained by the PPBE process, the program is already in potential jeopardy before arriving in the request for proposal (RFP) stage.

The budgeting issue often escalates during the RFP stage. Contractors oftentimes base their proposal estimates using historical actuals with inflation factors built in for time and manpower. However, since not reporting overtime is a common problem, these so called actuals often do not reflect all hours truly expended on difficult tasks in past projects. Furthermore, the accuracy of the historical data is also dependent on whether or not progress was tracked and reported on a daily basis and many organizations are challenged by the lack of an automated time-reporting system. All of which can result in underestimating the duration of tasks that are then used to generate the project cost estimate.

If the contractor bases their proposal on the budget allowance knowing that it cannot be met, then they may be relying on making up the shortfalls later on in their negotiations for requirements changes. The negative implications of underbidding based on a budget allowance can further be compounded after the contract is awarded. In this case, the contractor may implement the program at the funded/proposed amount and then reduce all the budgets by 10 to 15 percent to create a management reserve in time and budget to allow for the unexpected. Ideally, the contractor would have accelerated the schedule to create a schedule reserve and shorten the length of the program to fund the budget reserve. However, contractors are often unable to accelerate the schedule because sufficient funding (or personnel) is unavailable to support an earlier schedule.

Program Execution Challenges

Program execution comes with many challenges with technology, staffing, schedules and budgets. One of the biggest chal-

Table 2: *Planning Cycle*

Phase	Phase Defined
Phase 1: Planning	The DoD assesses capabilities, analyzes the threat and national defense policies and develops resource informed program guidance. This guidance defines the requirements for the military services.
Phase 2: Programming	The services translate guidance into a plan to allocate resources to accomplish mission requirements. They cost out force objectives six years in the future.
Phase 3: Budgeting	The President's budget is prepared, reviewed, and sent to Congress. This phase concentrates on the funding requirements necessary to do the job.
Phase 4: Execution Review	Assessments are made concerning current and previous resource allocations and whether the DoD achieved its planned performance goals. Services apply performance metrics to ascertain whether appropriate allocation of resources exist in current budgets. Recommendations may be made to replace a program with alternative solutions or make funding adjustments to correct resource imbalance if performance goals are not being met.

lenges is to react to changes, such as requirements creep, without losing control of the program.

When changes or problems surface that require a modification to the schedule, adjusting the program baseline can pose a real challenge. There are several reasons for this. For the contractor, a change request must be internally coordinated to check feasibility. It is often a challenge to gather all the required people to analyze the impact of the change within the project and across other projects to determine if the staffing available can support the revised plans. Once the contractor has developed a new baseline with the change, the contractual process will create a lag. It can take weeks or months to get a change request approved. Scope and schedule changes often require coordinating handoffs between several organizations before agreeing on new delivery dates. Since it is unusual to stop a program while you are re-baselining, the project team continues to track against the original baseline that is in reality obsolete while the approval process is taking place. Continuing to track against an obsolete plan impedes effective management because true priorities become lost which can then lead to the misallocation of resources.

In order to validate that the program can be completed within the contract requirements, EVM system descriptions require a schedule. The larger programs typically require a schedule with logical ties between the tasks (often a *critical path method* schedule) as opposed to the simpler schedule without links between the tasks. The PM can base the program network schedule on the resources available or assume that management will get the resources in time for the program to be successful. Neither approach is ideal since the non-availability of the right resources can delay the program and even a schedule that uses resource allocations to determine the durations makes assumptions about the availability of resources needed in the future. In addition, program contract leaders have to develop program plans around the available funding constraints in terms of both amount and timing of cash flow. Lack of sufficient funding prevents contractors from developing schedules optimized for best cost, schedule, or resource availability and thereby results in a more inefficient plan.

Recommendations
At the Strategic Level
If the true intent of OMB's implementation of EVM is to better manage IT pro-

jects' cost, schedule, and performance to maximize benefit for the taxpayer dollar, then the entire operating environment in which EVM is implemented will need transformation as well. EVM can track progress of a project, but it cannot solve the underlying systemic issues that created an underfunded/underbid project budget that inadvertently puts the project at high risk from the outset.

Agencies can take steps to practice more realistic project portfolio management in order to identify duplication of effort in attempts to gain desired capabilities. This would promote cross leveling to enable more adequate funding of projects that remain in the portfolio. Agencies can also leverage system engineering tech-

> *"The negative implications of underbidding based on a budget allowance can further be compounded after the contract is awarded. In this case, the contractor may implement the program at the funded/proposed amount and then reduce all the budgets by 10 to 15 percent ..."*

niques to divide the project into smaller parts to enable a more agile response to changes.

Because agencies must meet 90 percent of agency goals for cost, schedule, and performance in order to achieve green on the President's Management Agenda scorecard, there will be cultural pressure to view the EVM process as a contractual requirement that is administered with audit-like rigor by the review teams. Accommodating extensive government certification reviews, collecting and arraying data in prescribed categories, and preparing detailed reports requires time, effort, and cost to the government and can draw some of contractor engineering resources away from program execution.

Efforts should be made to counter this cultural pressure to ensure that tailored EVM requirements remain tailored and do not become overly cumbersome. The Government Accounting Office (GAO) found that commercial firms that use EV systems produce reports more frequently, more quickly, and in less detail than traditionally found in the DoD [12]. The focus should be on the information the EVMS is communicating and less on the presentation itself. This will enable program management to identify the areas that need program management attention and develop corrective actions needed to achieve program success.

At the Organizational and Project Levels
All levels of program management (oversight, management, and execution) need to understand the principles of EV, but more importantly they need to understand human behavior. A good PM will anticipate reluctance and will prepare to employ savvy political strategies to solicit buy-in. By emphasizing that the EVMS is aimed at improving the overall program progression to successful completion on time and on budget and by understanding the impacts of their behavior, management can positively influence the team to do their best. However, the PM must be realistic and cannot deny the challenges of implementation with the team.

In overcoming those challenges of implementation, training is key. This training must include the oversight authorities. This will help them understand and trust the signals that the EVMS is sending so they respond in a timely manner when issues are raised such that the situation does not become unrecoverable. Training in the concepts of EV should include practice in developing project schedules with different styles of work breakdown structures (execution oriented vs. product oriented) to demonstrate which orientation style works best when changes occur and what level of detail to plan. Too much detail makes the system burdensome – too little and it lacks credibility. In developing these work breakdown structures, project members should acknowledge and anticipate that later life-cycle activities, such as testing, will have different cost/schedule variances than earlier life-cycle activities. The goals of effective program execution need to be emphasized during the training. Questions to answer during the training sessions might include the following:

1. If work is tracked at a high level, can the details be used to sum up to the

total? If not, how can the high-level work completed be assessed?

2. How will the plan work in practice?
3. What happens if the plan changes?

EVM requires truth telling [13]. It often involves reporting contentious facts, delivering bad news, and sharing difficult feedback. Some areas in which interpersonal relations training may help the team are the following:

1. Communications.
2. Leadership.
3. Active Followership.
4. Emotional Intelligence.

Once the team has been trained, then the PM must create and diligently maintain a culture of execution. Strategies to accomplish this might include the following:

- **Celebrating success.** People respond to positive reinforcement. When the team's efforts result in a big win for the project, celebrate! Celebrating success builds team spirit and encourages repeat performance. Make sure the success is public knowledge. Share it with the entire organization, if possible. Making public heroes out of those responsible for the success is likely to encourage others to strive for their chance in the limelight.

- **Being a role model.** The PM must personify the principles of the EVM process in every interaction. If you do not practice what you preach, how can you expect it of your team? Speaking candidly, insisting upon realistic information, focusing on results and being actively involved in the success of the project makes the PM a great role model for the project team. When the team submits undesirable, but realistic numbers, the PM must remain cool. Candid communication and realistic information are cornerstones of an EVMS. PMs must remain calm and then try to find out what happened and how the project can be brought back on track. The PM must be accessible and available to the team on a regular basis.

- **Encouraging appropriate behavior.** EVM in action is not always easy. Speaking candidly and using realistic data comes with risk. The PM can encourage the team to do so by praising them when they are bold enough to present realistic numbers, even when doing so makes them and the project look bad. Acknowledge them for speaking their minds and communicating project challenges.

Organizational leaders and PMs must keep in mind that what you measure is important – what you pay attention to and focus on tends to get reinforced whether or not it enhances project progress. Counting missed milestones and focusing on the negative can result in an overemphasis on doing tasks on time against a plan that may be out of date. If the program only measures missed milestones instead of keeping the emphasis on the final goals (focusing on the positive), near term tasks may receive a disproportionately high priority to increase the number of tasks completed. However, the best approach for the long term may have been to miss some near-term tasks to take advantage of resources available now but which another program will require at the same time if the tasks are performed in the order of the original plan. If innovation and creativity are stifled because of a culture that punishes managers who have

---

> *"The PM must personify the principles of the EVM process in every interaction. If you do not practice what you preach, how can you expect it of your team?"*

EV variances, the goal of improved program execution by implementing EVM will not be met.

Making EVM Work for You and Your IT Project

One sociological definition of technology is *a set of standardized operations which yield predetermined results* [14]. The more likely predetermined results occur, the stronger the technology. Developing software does not have the predictability of outcome as manufacturing processes do. Many people would argue that developing software programs and information systems is just as much art as it is science. While style guides can be implemented to maintain some consistency, two different programmers can still approach the same requirement very differently obtaining the same results via very different coding paths. Predicting, replicating, and standardizing those thought patterns that created those coding paths is very difficult. As such, apply-

ing EVM can be more challenging in IT projects. Nevertheless, most experts today agree that EVM is suitable for managing major IT projects [1].

With this in mind, PMs should carefully consider exercising their discretion in applying EVM. Ultimately, the decision will largely be subjective based on how the cost-benefit analysis is conducted. Therefore, the value the PM gets will be determined by how EVM is implemented, taking care to avoid unnecessary cost drivers, such as the following:

- Lengthy *systems descriptions* of EVMS [15].
- Written variance analysis at the control account level [15].
- Over-specified work breakdown structure [15].
- Over- or under-compensating for inevitable planning errors [16].

Fleming and Koppelman offer sound advice in the June 2006 issue of CROSS-TALK on how to pragmatically obtain the benefits of EVM using *simple* EV without overtaxing the project team [17].

Tracking project progress should be a continuous activity where data is collected as the activity occurs. Thus when EVM is optional, PMs should seek as close to real-time data as possible directly from the contractor in whatever format the contractor uses, as long as the format remains consistent and the data is accurate and verifiable.

The following set of questions can assist a PM in developing a tracking and measurement program:

- What visibility do you have in terms of resources, time, and cost?
- What can you track and measure? How often can you do it?
- Who sets the standards for performance? How realistic are they? How clear are they? Do these standards contribute to project goal achievement?
- How often do you need to report and to whom? How long does it take to prepare the reports?
- What performance variance is acceptable? At what level of variance is action required?
- What rewards and penalties are available?
- What is the criticality of the system being developed?
- What is the critical path for the system being developed to be operational?

A good PM knows metrics are just one of many tools of the project management tool set. When a healthy balance and perspective is maintained by using EVM as a management tool rather than a financial report card that supersedes all other

tools, the benefits of EVM become more apparent.

Given the imperfect world in which we operate in the DoD and the federal government, can EVM by itself achieve the goal of avoiding costly IT failures? Probably not. EVM will not prevent requirements creep or contractors underbidding projects based on budget allowances, or poorly planned projects. However, by managing its adoption through cultural modifications and training, it is a step in the right direction.◆

References

1. Olsen, Florence. "EVM Sounds the Alarm: Smart Agencies Let Earned Value Management Lead Them to Better Program Management." Federal Computer Week 16 Mar. 2006 <www.fcw.com/article92541-03-13-06Print>.
2. CIO. A Framework for Developing Earned Value Management Systems (EVMS) Policy for Information Technology (IT) Projects. Washington: CIO Office, 2005 <www.cio.gov/documents/Framework_for_Developing_EVMS_Policy_ 12-5-05.pdf>.
3. Evans, Karen. Improving Information Technology Project Planning and Execution. Washington: Office of Management and Budget, 2005.
4. Federal CIO Council. A Framework for Developing Earned Value Management Systems Policy for Information Technology Projects. Washington: CIO Office, 2005 <www.cio.gov/documents/Framework_for_Developing_EVMS_Policy_12-5-05.pdf>.
5. Wynn, Michael. Revision to DoD Earned Value Management Policy. Washington: Undersecretary of Defense for Acquisition, Technology, and Logistics, 2005 <www.acq.osd.mil/pm/currentpolicy/EVM%20Policy%20letter%203-7-05.pdf>.
6. DoD. Defense Acquisition Guidebook. U.S. DoD, 2006 <http://akss.dau.mil/dag/Guidebook/IG_c11.3.1.asp>.
7. Rogin, Josh. "No One-Size-Fits-All Approach for EVM." Federal Computer Week 10 July 2006 <www.fcw.com/article95183-07-10-06-Print>.
8. Federal Register 5 July 2006 <http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5966.htm>.
9. Rogin, Josh. "FAR Gives Agencies Wiggle Room." Federal Computer Week 5 July 2006 <www.fcw.com/article95156-07-05-06-Web>.
10. Thormeyer, Rob. "Agencies Struggle With EVM as OMB Deadline Approaches." Government Computer News 3 Nov. 2005 <www.gcn.com/vol1_no1/daily-updates/37486-1.html>.
11. Mosquera, Mary. "What's the Future of Your IT Project?" Government Computer News 22 Aug. 2005 <www.gcn.com/24_24/news/36698-1.html>.
12. United States. GAO. Significant Changes Underway in DoD's Earned Value Management Process. GAO/NSIAD-97-108. Washington: U.S. General Accounting Office, May 1997 <www.gao.gov/archive/1997/ns97108.pdf>.
13. Harris, Lynn, and Jeff Arnold. "Truth Telling: Confronting the Reality of Lack of Candor Inside Organizations." In Transition 2006.
14. Freeman, David. "People, Technology, and the Environment." Colorado State University, Fall 1998 Semester.
15. Christensen, David. S. "The Costs and Benefits of the Earned Value Management Process." Acquisition Quarterly Fall (1998): 373-385 <www.suu.edu/faculty/christensend/cbaevms.pdf>.
16. ASK Process, Inc. "Using Earned Value Part II: Tracking Software Projects." Ask Process (2003) <www.askprocess.com/Articles/UsingEV2.pdf#search=%22Using%20Earned%20Value%20Part%20II%3A%20Tracking%20Software%20Projects%22>.
17. Fleming, Quentin W., and Joel M. Koppelman. "Start with 'Simple' Earned Value on All Your Projects." CROSSTALK June 2006. <www.stsc.hill.af.mil/CrossTalk/2006/06/0606FlemingKoppelman.html>.

Notes

1. The MDA's primary responsibility is to make decisions on whether the programs should be initiated and whether they should proceed through the various phases of the acquisition life cycle. At each major decision point, the MDA must determine whether the program, or a key increment of the program, should be terminated, modified, or approved to proceed.

2. Infostructure is an Army Network Enterprise Technology Command term used to describe the enterprise-managed IT infrastructure that is part of the Global Information Grid.

About the Authors

LTC Nanette Patton is currently serving as a program analyst in the Office of the Surgeon General (OTSG). She recently completed a one-year fellowship at the RAND Corporation. Patton has eight years experience as a health services systems manager and is Level III DoD-Acquisition certified in Information Technology and Level II certified in Program Management. She has a master's degree in human resources management from Chapman University, and a Master of Business Administration in computer information systems from Colorado State University.

OTSG
PA&E Manpower
5109 Leesburg Pike
Skyline 5, RM 598
Falls Church, VA 22041
E-mail: nanette.patton@us.army.mil

Allan Shechet is president of Savvy Services Incorporated, a project management consulting company and has more than 20 years experience with EVM systems in Aerospace and IT companies. He has a master's degree in organization development from Fielding Graduate University, is certified as a Project Management Professional by the Project Management Institute (PMI), and is an active volunteer for the Los Angeles chapter of PMI.

Savvy Services
2239 Linnington AVE
Los Angeles, CA 90064
Phone: (310) 720-2522
E-mail: allan@savvyservices.net

Challenges of Internet Development in Vietnam:
A General Perspective

Duy Le
College of William and Mary

Dr. Rayford B. Vaughn and Dr. Yoginder S. Dandass
Mississippi State University

This is a report on the evolution of a robust internet infrastructure in the developing nation of Vietnam. Given Vietnam's history and its evolution under communist rule, readers may be interested to now learn about Vietnam's Internet evolution and its concern with security, government control, and long-range plans. While significant progress has been made throughout the nation, much remains to be done. The material for this article was gleaned from Vietnamese documents and open source materials.

Computer networking and security is an important concern in most countries, including developing nations like Vietnam. While the Vietnamese economy is under-developed compared to Southeast Asia as a whole, its information technology infrastructure is growing rapidly. However, its developing economy and new technologies have introduced issues and concerns (e.g., computer engineering, network security, software engineering, and e-commerce) that are being addressed today by policy makers. This article provides an overview of the Internet infrastructure deployment activities and the evolution of computer security policies in Vietnam from 1997 to the present.

The Vietnamese government has been focusing on improving the information communication technology (ICT) of that country in order to keep up with other parts of the world. The government is actively supporting specific activities such as encouraging public and private sectors to participate in the deployment of the Internet; increasing investments by foreign ICT companies; adopting new, modern technologies; and stimulating domestic research. Initially however, development of ICT was not a governmental priority and caused the Vietnamese ICT industry to lag behind their southeast Asian counterparts. It took nearly five years – from 1997 when Vietnam obtained its first international Internet connection until 2002 – for the government to recognize the potential of ICT. The Ministry of Posts and Telematics (MPT), the highest technological government organization, was established in 2002 and began drafting policies and regulations designed to exploit this technology for economic and industrial use and to incorporate the Internet into Vietnam's cultural landscape. According to the MPT, growth of ICT in Vietnam is projected to keep pace with other countries in the region such as China, Singapore, and Korea and to be on par with the West by 2010.

Initial Development of the Internet in Vietnam

This section presents the development of ICT and the impact of the Vietnamese government's policies (or lack thereof from 1997 until 2005) on the deployment of ICT from 1997 onwards.

Roadblocks to Development

Early efforts to provide Internet service in Vietnam had to overcome several roadblocks. For example, in 1991, negotiations between an Australian university and the Hanoi Institute of Information Technology (the governmental organization dealing with networking problems in 1990) were unsuccessful. In 1996, the Vietnam government decided to delay the implementation of the first international Internet connection for general, non-governmental use because of a perceived lack of suitable rules and regulations required to control the new technology. In December of 1997, after the government issued a flurry of decrees and resolutions outlining how the Internet was to be used and controlled, Internet service providers (ISPs) were permitted to offer commercial Internet access [1, 2].

As illustrated in Figure 1, the growth rate in the number of subscribers was more than 100 percent each year. However, there were only approximately 100,000 subscribers and only 200 leased Internet lines in 2001, indicating low Internet usage by businesses and educational institutions. This was primarily because the government favored establishing regulatory control of the Internet through government-owned companies versus promoting a competitive market comprised of private companies. As a result, there were only four ISPs in Vietnam. Of these, Saigon Postel Corporation was the only private company. Furthermore, only the government-controlled Vietnam Data Communication (VDC) company was permitted to provide international connectivity [2, 3]. In 2001, the total international bandwidth through VDC was approximately 34 Mbps.

The initial Internet infrastructure was designed to accommodate e-mail and Web services over dial-up and leased lines with-

Figure 1: *Users Estimated on the Basis of Two Users Per Subscriber (Adapted From* [1]*)*
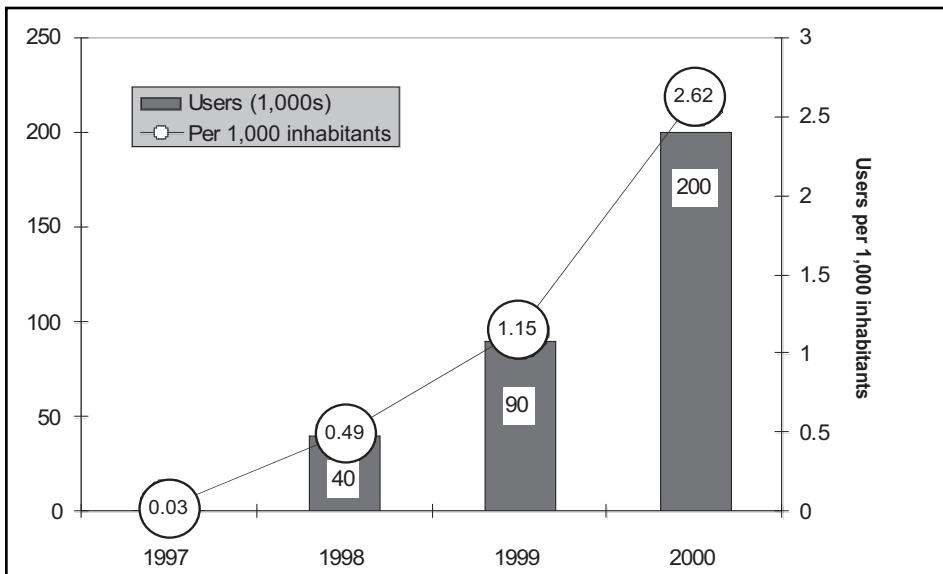
out concern for modern services such as high-speed and wireless Internet access and high-quality multimedia applications. This made deploying and applying new services, such as video-on-demand and distance learning relatively difficult [4]. The notion of quality of service became a concern towards the end of 2001, after public complaints related to lack of speed, stability, security, flexibility, and general services began to surface.

Topology and Structure

The overall network was designed centrally by the government to have a dual-layered architecture. The upper layer, called the Internet Access Point (IAP), is directly controlled by the government. The lower layer, called the Internet Service Point may be controlled by commercial entities. All network providers must follow and implement this architecture. The layers are described in detail as the following:

- **IAP.** The IAP layer provides the interface between the domestic network and the Internet at three main access locations: Ho Chi Minh City, Hanoi, and Danang. The IAP was designed to operate as a high-performance national core network. The main function of the IAP is to route all incoming and outgoing traffic between the outside Internet connections and the lower service point layer. The IAP layer also implements a cache system to increase the flow of incoming traffic and a firewall system to filter incoming and outgoing traffic.
- **Internet Service Point.** At least 57 of Vietnam's 61 large towns and cities must be covered by this layer, according to government policy. Typical Internet services, such as e-mail, Web page, and value-added services are provided at this layer. A firewall system is also placed at this layer to protect the national network and is managed by the IAP.

The information content services provided to users depend on the capabilities of individual ISPs. These services are classified into the following two groups for security management: content services and financial services. Content service includes popular services such as the Domain Name System, proxy, File Transfer Protocol servers, chat, Web, news, e-mail, and directory. Each service is required to have at least one protection system which is separate from the protection systems of other services. Two independent firewall systems are installed to manage control between content services and financial services. Financial services

are separately operated and administered in order to provide enhanced security and reliability.

Although the IAP served as the core of the national network and its security was supported by an extensive firewall system at each node, the system was still subject to vulnerabilities. In 2002, concerns were expressed within the government over the possibility of private entities establishing international connections outside of direct government control (e.g., via satellite links). Furthermore, it was becoming evident that the current architectural and control structure was not conducive to the rapid expansion of Internet activity (there were still just four main providers of Internet service).

Modernization of Vietnamese ICT

In 2002, the MPT was created as the single agency responsible for Internet development and control in Vietnam. Today, the

---

"Flexibility to enable interconnection of networks from disparate segments of the Vietnamese Internet markets ... has been the central goal of the NGN standard."

MPT remains the highest level government organization that regulates and administers the development of Vietnam's ICT.

Modernization Initiatives

The MPT has initiated significant actions in order to improve Vietnam's ICT and to promote technological development. The initiatives include the following:

- Developing and implementing a plan for developing Vietnam's Internet services [2] with the following three objectives: 1) to promote the deployment of high quality Internet connectivity in all economic, cultural, social, security, and defense activities at a cost comparable to those of other countries in the region; 2) to develop the national network infrastructure into an application environment conducive to all forms of online services (e.g., trade, administration, finance, banking, mass

media, and education); 3) to create a competitive environment for public and private enterprise in terms of providing Internet exchange services, access services, and online services.

- To integrate the national data network with the networks of commercial providers while allowing the government to manage and regulate control at a high level [5] and to supplement and modify the regulations that had been in place since 1997 as necessary [2].
- To regulate and apply the latest technologies for public use and to provide these technologies at the highest level of quality. Today, ISPs must obtain quality certificates from the Department of General Post and Telecommunications, must abide by certain service parameters, and must provide quarterly reports of service to the government.

Government oversight has helped usher in a new period of ICT development in Vietnam. Currently there are four IAPs (two of these are private enterprises). As Figure 2 (see page 18) illustrates, the number of ISPs has increased from four in 2002 to eight in 2005 (four of these are public enterprises). Additionally, a large number of Internet content providers have been granted a license to operate. Although government-controlled ISPs still maintain a majority of the national ICT market, Internet use in Vietnam is growing as illustrated by the following statistics from 2005:

- Number of Internet users: 8,560,799.
- Internet users as a percentage of the national population: 10.31 percent.
- International connectivity bandwidth: 2,997 Mbps.
- Number of domain names assigned (.vn is the top-level domain for Vietnam): 12,611.
- Number of IP address assigned: 607,744.

Modern Internet Infrastructure

The government has also proposed the New Generation Network (NGN) as the standard for the modern national network infrastructure. The backbone layer of this model is organized into the following two levels:

1. **National core backbone.** Using multi-protocol label switching technology for switching between the three main nodes at Ho Chi Minh City, Hanoi, and Danang, this level serves as the core national network. For this reason, it must guarantee gigabyte switching speed, high-level security, extensibility, and recovery functions.

2. **Regional backbone.** This level receives and forwards all traffic transferred between end-users and the national core backbone network. As an intermediate level, it must also guarantee security, stability, and congestion recovery during periods of peak usage. Flexibility to enable interconnection of networks from disparate segments of the Vietnamese Internet markets (e.g., ISPs, universities, banks, and mass media) has been the central goal of the NGN standard. This is in direct contrast with the closed, non-standard, small scale, network infrastructure with poor quality and security that was initially deployed between 1997 and 2002.

Network and Computer Security Concerns

The appearance of the first Vietnamese hackers in 2001 did not initially cause concern among the ISPs and financial institutions [7]. However, the Vietnamese government began to take notice of security vulnerabilities when hacker groups discussed the vulnerabilities of Vietnam's Internet infrastructure on a large scale in 2002 [8]. In a workshop in November 2002, Vietnamese hackers provided evidence of their penetrations into important systems such as the billing systems of Hanoi Telecom Company (the largest local provider of telephone lines) and the VDC Company (the national ISP). Furthermore, more than 80 percent of the Web site for domestic companies (e.g., The Bank for Foreign Trade of Vietnam, a large Vietnamese bank) had been penetrated. This workshop and additional security problems from domestic hacking from 2001 to 2003 influenced the government to make internal networks more secure. In June 2004, the government formally introduced a directive for the assurance of safety and security for postal, telecommunication, and Internet information [2]. This directive focused on the following three main points:

- The guarantee of information and communication for the party, state agencies, and the armed forces.
- Controls on the procurement of equipment needed to safeguard postal and telecommunication networks and all functions under their management control.
- Halting ICT services in coordination with the Ministry of Public Security during instances of national violence or riots, and when the use of postal, telecommunication, and Internet services threaten to infringe upon national security is detected.

In reality, not all providers are qualified to meet the security standards issued by the government that the public and private national network providers are expected to follow. Furthermore, certain providers also ignore security standards when required in order to improve the performance of their networks. Therefore, instead of striving to completely satisfy the government's security requirements, most providers comply as best they can. Because of this, resolving computer security and information assurance problems is still a major challenge faced by Vietnamese ICT officials, providers, and users.

Another roadblock to secure computing in Vietnam is the lack of personnel trained in computer and network security. In an effort to improve its software development capability (using India as a model), the Vietnamese government has focused on producing software engineers. The training of personnel and research and development of security engineers in cooperation with Vietnamese educational institutions has not been a priority. Currently, there are only three network and Internet training centers (operated by Cisco) [6], one each in Ho Chi Minh City, Hanoi, and Danang. This is in contrast to the nearly 100 software development centers around the country. The high cost of establishing and operating training centers has also been an inhibiting factor. As a result, there are approximately 13 Vietnamese Cisco Certified Internetworking Experts with security training of which only a few are helping the government resolve network security issues.

Recognizing the importance of secure networks, the government is now beginning to address security issues. In 2004, Vietnam established IPv6 links with Japan in order to research and experiment with the new services available in IPv6 [9]. The government also began the construction of the Internet Data Center (IDC) of Vietnam that is expected to be completed by 2007 [10]. The IDC will be the central location that will connect the Vietnamese Internet infrastructure to the international Internet (an unsecured environment). The IDC will be a challenge for the MPT because the IDC will have to satisfy the security and operational requirements of the Vietnamese government and commercial entities as well as the requirements of foreign partners [5, 10].

Conclusion

The material presented in this article is specific to Vietnam. However, the difficulties encountered by the Vietnamese government in balancing the conflicting needs of establishing tight control over access and content while simultaneously promoting the economical, educational, and cul-

Figure 2 A and B: *Comparison of the Vietnamese Internet Market* [2, 6]

(A) ISP market share in November 2002
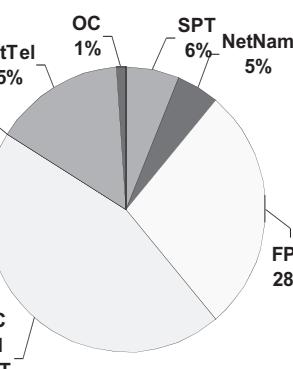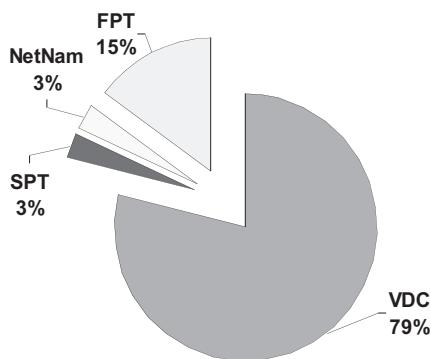
(B) ISP market share in September 2005

ISP Name	Region
FPT: Financial Promoting Technology Corporation	Countrywide
HPT: Hanoi Post and Telecommunications Company	Northern Vietnam
NetNam: NetNam Company	Northern Vietnam
OC: One Connection	Southern Vietnam
SPT: Saigon Postel Corporation	Southern Vietnam
VDC: Vietnam Data Communication Company	Countrywide
VietTel: VietTel Comany	Northern Vietnam
VNPT: Vietnam Posts and Telecommunications Company	Countrywide

ISP service regions in 2005

tural use of the Internet can be generalized to other developing communist nations. It is interesting to study the control structures and the regulatory environment established in Vietnam. The Vietnamese government has an ambitious agenda for establishing a modern Internet infrastructure while simultaneously exercising governmental control on international connectivity and content. Learning from its mistakes that hampered the early adoption and growth of the Internet in Vietnam, the government is now actively engaged in activities such as the planned growth of the national network, construction of new network connections, extension of interconnectivity with other countries, and improvement of software development capabilities.◆

References

1. Kelly, T., et al. "Vietnam Internet Case Study." Geneva, Switzerland: International Telecommunication Union, 2003.
2. Ministry of Post and Telematics. "Legal Documents of the Vietnam Ministry of Post and Telematics." <www.mpt.gov.vn/english/legal_doc/?thucdon=ld>.
3. Nguyen, T.H. "Internet Governance for Socioeconomic Development Case Study From Vietnam." Report of Global Internet Policy Initiative Vietnam. 2005 <www.wgig.org/docs/case%20study%20from%20Vietnam.ppt>.
4. Materi, R.R., and P.J. Fahy. "Interim Report: A Case Study of Internet-based Distance Education Program Development in Vietnam." International Review of Research in Open and Distance Learning. Apr. 2004.
5. Nguyen, L.T., H.B. Quy, and Lo. T. Nguyen. "Development Plan of Internet Vietnam (Phase I, II, III, and IV)." Planning Report of Vietnam Post and Telecommunication Corporation – VNPT. Hanoi, Vietnam: Jan. 2005.
6. Vietnam Internet Center. "Statistical Data of Internet Vietnam." Nov. 2005 <www.vnnic.net.vn/thongke/thongke/jsp/trangchu/index.jsp>.
7. Van, B. "The First Attack of Vietnamese Hackers Through Domestic Companies in May 2001." VNExpress: May 2001 <http://vnexpress.net/Vietnam/Vitinh/2001/05/3B9B07CD>.
8. VietnamNet. "The First Vietnam Hacking Workshop." Nov. 2002 <www.vnn.vn/cntt/xalo/2002/11/212581>.
9. Nguyen, L.T., D. Le, and L.H. Vu. "Planning and Performance Evaluation an IPv6 Experimentation Network in Vietnam." Hanoi, Vietnam: Vietnam Posts and Telecommunications Institute of Technology, Apr. 2003.
10. Nguyen, L.T., and Lo.T. Nguyen. "Development Plan of Internet Data Center (IDC) in Vietnam." Planning Report of Vietnam Post and Telecommunication Corporation – VNPT. Hanoi, Vietnam: June 2005.

About the Authors

Duy Le is currently a doctoral student in Computer Science at the Department of Computer Science of the College of William and Mary. Before of that, he was at Mississippi State University (MSU) to work with Dr. Ray Vaughn and Dr. Mahalingam Ramkumar in computer security and at the University of Massachusetts, Amherst with Professor Jim Kurose in sensor network. His research interests include the wireless network and performance evaluation of the computer network .

Computer Science Department
College of William & Mary
P.O. Box 8795
Williamsburg, VA 23187-8795
Phone: (757) 221-3484
Fax: (757) 221-1717
E-mail: duy@cs.wm.edu

Rayford B. Vaughn, Ph.D., is the Billie J. Ball Professor of Computer Science and Engineering at MSU where he teaches and conducts research in the areas of software engineering and information security. Prior to joining the University, he completed a 26-year career in the U.S. Army, retiring as a Colonel, and three years as a vice president for Defense Information Services Agency Integration Services, EDS Government Systems. Vaughn has more than 100 publications to his credit and is an active contributor to software engineering and information security conferences and journals. In 2004, he was named a MSU Eminent Scholar. Vaughn received his doctorate from Kansas State University in 1988.

Billie J. Ball Professor of Computer
Science and Engineering
Director, Center for Computer
Security Research
P.O. Box 9637
Mississippi State University
Mississippi State, MS 39762
Phone: (662) 325-7450
Fax: (662) 325-8997
E-mail: vaughn@cse.msstate.edu

Yoginder S. Dandass, Ph.D., is an assistant professor of computer science and engineering at MSU. His research interests include high performance computing, reconfigurable computing, and computer security. Dandass was a research associate at MSU from 1997 to 2003, and was an information technology consultant from 1989 until 2007. He received his doctorate in 2003 from MSU and his master's degree from Shippensburg University in 1996.

Department of Computer
Science and Engineering
P.O. Box 9637
Mississippi State University
Mississippi State, MS 39762
Phone: (662) 325-7502
Fax: (662) 325-8997
E-mail: yogi@cse.msstate.edu

Net-Centric Operations: Defense and Transportation Synergy

COL Kenneth L. Alford, Ph.D., and Steven R. Ditmeyer
National Defense University

The Department of Defense (DoD) is actively working to transform platform-centric operations into net-centric operations. Net-centric railroading could provide DoD's Strategic Rail Corridor Network (STRACNET) with unified operations in which positioning systems, sensors, computers, advanced mathematical models, and digital communications could be used to collect, process, and disseminate information to improve the safety, security, and operational effectiveness of our nation's railroads in support of national defense. As both departments pursue net-centric operations there will be numerous opportunities to share technology and experience.

Admiral Jay Johnson, Chief of Naval Operations, apparently coined the phrase *net-centric warfare* in 1997[1]. Net-centric warfare has been defined as *an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization* [1].

Rapid and significant advances in information technology hardware and software during the past two decades have made it possible to fundamentally change the way information is gathered, stored, processed, and used. As the DoD Chief Information Officer (CIO), John G. Grimes, recently noted:

> … We must recognize that it is all about information, and we must view information as a strategic asset. Timely, accurate and trusted information lies at the heart of net-centric operations. [2]

The concept of net-centric operations, though, is not limited to warfare and the DoD. The DoD is not the only large government organization that is considering moving to net-centric operations. The Department of Transportation (DoT), for example, is seriously evaluating and encouraging net-centric railroading.

Net-Centric Railroading

Intelligent railroad systems were first described in the Secretary of Transportation's report, *The Changing Face of Transportation*[2], published in 2000, and their description was expanded in the Federal Railroad Administration's (FRA) *Five-Year Strategic Plan for Railroad Research, Development, and Demonstrations*[3], a March 2002 congressional report.

The FRA, railroads, and the railroad supply industry have been working on the development of intelligent railroad systems for command, control, communications, and information (C3I), as well as for braking systems, grade crossings, defect detection, and planning and scheduling systems. These technologies can prevent collisions and overspeed accidents, prevent hijackings and runaways, increase capacity and asset utilization, increase reliability, improve service to customers, improve energy efficiency and emissions, increase economic viability and profits, and enable railroads to measure and control costs and *manage the unexpected* [3].

Intelligent railroad systems could enable railroads to improve their quality of operations on the DoD-designated Strategic Rail Corridor Network[4] (STRACNET), enhancing their responsiveness to military deployments. They would also enable railroads to respond with flexibility and agility to rapid changes in the transportation marketplace. These systems could alleviate the need for a division commander to call railroad executives late at night to find out the location of railroad cars for loading their division's heavy equipment – like Maj. Gen. David Petraeus had to do during the 101st Airborne Division's deployment to participate in Operation Iraqi Freedom [4].

Benefits of Net-Centric Operations

Proponents of net-centric operations – in government, industry, and academia – claim many benefits. Here are some of the most frequently claimed benefits that should apply to the DoD, the DoT, and the railroad industry:

1. Increased operational flexibility.
2. Increased decision-making speed.
3. Cost savings through increased efficiency of asset usage.
4. Improved support to geographically dispersed elements.
5. Increased visibility and a better understanding of operations.
6. Self-synchronization of subordinate organizations. For the DoD, self-synchronization means *the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up. … Self-synchronization is enabled by a high level of knowledge of one's own forces, enemy forces, and all appropriate elements of the operating environment* [1].
7. General benefits that result due to increased connectivity. *Net-centric computing is governed by Metcalfe's Law, which asserts that the* power *of a network is proportional to the square of the number of nodes in the network. The* power *or payoff of net-centric computing comes from information-intensive interactions between very large numbers of heterogeneous computational nodes in the network* [1].

Net-Centric Railroad Technologies

Like the DoD's concept of net-centric warfare, the DoT's concept of net-centric railroading is a *system of systems*. Twenty-nine key technologies, programs, and systems, either developed or under development, have been identified which could help create a net-centric railroading system. (For a complete list, please see the sidebar entitled *Railroad Net-Centric Technologies*.)

Here are 10 of the many technologies that are being considered for incorporation into a net-centric railroading system. Some, or all, of these systems may have direct application for the DoD, as well:

- **Positive Train Control (PTC) systems** are integrated C3I systems for controlling train movements with safety, security, precision, and efficiency. PTC systems would improve railroad safety by significantly reducing the probability of collisions between trains, casualties to roadway workers and damage to their equipment, and overspeed accidents. The National Transportation Safety Board (NTSB) has had PTC on its *most wanted* list of

transportation safety improvements since 1990[6]. PTC systems are comprised of digital data link communications networks, continuous and accurate positioning systems, on-board computers with digitized maps on locomotives and track maintenance equipment, in-cab displays, throttle-brake interfaces on locomotives, data-link connections at switches (both powered and manual) and wayside detectors, and train control center computers and displays.

- **Crew alertness monitoring systems** promote on-duty alertness and vigilance of train crews through the use of non-invasive technology applications. Real-time monitoring and feedback of *individual alertness levels* would allow crew members to modify their behavior and reduce their risk of unsafe performance.
- **Crew registration and time-keeping systems** would use identification techniques such as the Department of Homeland Security's proposed Transportation Worker Identification Credential (TWIC), other electronic card keys, passwords, or biometrics such as fingerprints and/or retinal scans to ensure that only authorized crew members are permitted to control locomotives and track maintenance vehicles.
- **Locomotive health-monitoring systems** consist of sensors mounted on engines, traction motors, electrical systems, air systems, exhaust systems, and fuel tanks on locomotives. Most new locomotives are equipped with most of these sensors. In the future, the data would be transmitted over the digital data link communications network to train control centers, maintenance facilities, and motive power distribution centers to permit real-time monitoring of locomotive performance and efficiency, improved diagnosis of problems, and more effective assignment of locomotives to trains.
- **Wayside track sensors** are installed to identify a number of defects that occur on and alongside the track as well as identify conditions and obstructions along the track. Among the conditions and defects that could be detected are switch position, broken rail, misaligned track, high water, rock and snow slides, excessive rail stress, misaligned bridges and trestles, blocked culverts, and earthquakes.
- **Energy management systems (EMS)** are installed on locomotives to optimize fuel consumption and emissions. An EMS would receive information on track profile and conditions, speed limits, train length and weight, locomotive engine fuel performance characteristics, locomotive health monitoring systems, etc. Conceptual work has been done on EMS, but a prototype system has not yet been implemented.
- **Car on-board commodity sensors** are being installed on freight cars to monitor the status of the commodities being carried – measuring, for example, temperatures, pressures, vibrations, load position, radiation, gases, and biohazards.
- **Intelligent weather systems** consist of networks of local weather sensors and instrumentation – both wayside and on-board locomotives – combined with national, regional, and local forecast data to alert train control centers, train crews, and maintenance crews of actual or potentially hazardous weather conditions.
- **Security systems** consisting of closed-circuit television cameras and infrared presence detectors are being deployed at bridges and tunnels, and even on some locomotives, to provide detection of intruders and obstructions. Appropriate information would be transmitted via data link to train control centers and train and maintenance crews in addition to security forces.
- **Emergency notification systems** installed at train control centers provide for the automated notification of all involved organizations following railroad accidents, incidents, or threats. The implementation of net-centric railroading with intelligent railroad systems is not without impediments – the competition for capital within railroad companies, for example. Railroad companies need to understand, though, that a well-executed investment in intelligent railroad systems should reduce the capital needed for locomotives, cars, and tracks.

Net-centric railroading should enable railroads to manage unexpected situations by providing real-time information about current operations and the current environment. The DoD, as well as commercial railroad customers, could benefit significantly from improvements in visibility, running time, and service reliability resulting from the implementation of net-centric railroading.

Increasing Capacity

Today there is a capacity problem in railroading. During the past 25 years (following the deregulation of the railroad industry), American railroads have physically downsized – tracks, locomotives, train cars, and employees – while, at the same time, overall rail traffic has increased. With a growing economy and growing imports, railroads face congestion on many of their lines. The last time the nation faced a similar crisis was during World War II.

Net-centric railroading will provide an effective increase in capacity. It enables railroads to handle different types of traffic (such as coal, grain, container, and even passenger) that have different service requirements, enabling them to co-exist on the same facility. Different types of trains can each be managed according to their individual requirements.

Railroad Net-Centric Technologies

The accompanying article highlights several of the key technologies, programs and systems that can be incorporated in net-centric railroading. The following is the complete list:

- Digital data link communications networks.
- Nationwide Differential Global Positioning System.
- Positive train control systems.
- Electronically controlled pneumatic brakes.
- Knowledge display interfaces.
- Crew registration and time-keeping systems.
- Crew alertness monitoring systems.
- Track forces terminals.
- Automatic equipment identification.
- Wayside equipment sensors.
- Wayside track sensors.
- Locomotive health monitoring systems.
- Energy management systems.
- Vehicle-borne track monitoring sensors.
- Car on-board component sensors.
- Car on-board commodity sensors.
- Intelligent grade crossings.
- Intelligent weather systems.
- Tactical traffic planners.
- Strategic traffic planners.
- Yard management systems.
- Work order reporting systems.
- Locomotive scheduling systems.
- Car reservation and scheduling systems.
- Train crew scheduling systems.
- Yield management systems.
- Security systems.
- Emergency notification systems.
- Traveler's advisory systems.

These net-centric systems will enable control centers to know the location of all trains and the status of their performance, whether they are on schedule, behind schedule, or ahead of schedule. The tactical and strategic planning systems will enable railroads with flow control – similar to what the Federal Aviation Administration is able to currently do with aircraft – to anticipate the location of trains (two hours from now, four hours from now, etc.) and to initiate actions to reduce or remove congestion problems before they actually occur.

Sharing Insights

As the DoD continues to shift to net-centric operations, there is no reason that insights and lessons learned from work done thus far should not be shared with other federal agencies. The authors propose several concepts that may be beneficial to the railroad industry as they begin a net-centric transformation:

1. **Have a thorough discussion with the railroad industry regarding which information should be pushed to users and which information should be pulled by users.** The answers to those two questions are not necessarily disjoint data sets.
2. **Information security and information assurance must be part of every net-centric discussion.**
3. **Do not underestimate** the tension that exists between continuing investment in legacy systems and the upfront costs of replacement net-centric systems that offer a higher rate of return.
4. **Technological changes will affect the companies within the railroading industry in unforeseen ways.**

   …we must change how we train, how we organize, and how we allocate our resources … Because a net-centric force operates under a different, more modern rule set than a platform-centric force, we must make fundamental choices in at least three areas: intellectual capital, financial capital, and process. [1]

5. **The importance of redundant and back-up capabilities cannot be overstated.** A pessimistic look at history shows that failures often occur at the worst possible moment. The November issue of *Technology Review* provided an in-depth review of one such challenge during Operation Iraqi

Freedom. On April 2, 2003, Army LTC Ernest *Rock* Marcone (a battalion commander with the 69th Armor of the Third Infantry Division) led an armored battalion of almost 1,000 U.S. soldiers to seize Objective Peach – a key bridge across the Euphrates River and the last major obstacle before American forces would reach Baghdad. That night, Marcone's battalion was surprised by the largest counterattack of the war. All his net-centric sensing and communications technologies failed to warn him of the attack's scale. He did not realize that between 5,000 and 10,000 Iraqi troops with about 100 tanks and other vehicles were about to attack his position:

> *"Twenty-nine key technologies, programs, and systems, either developed or under development, have been identified which could help create a net-centric railroading system."*

Next to the fall of Baghdad, says Marcone, that bridge was the most important piece of terrain in the theater, and no one can tell me what's defending it. Not how many troops, what units, what tanks, anything. There is zero information getting to me. [5]

6. **Understand that your organizational culture will be affected by these changes.** One of the major lessons learned is that without changes in the way an organization does business, it is not possible to fully leverage the power of information [1].
7. **Maintain realistic expectations.** Metcalfe's Law is really about potential gains; there is no guarantee that simply hooking things up will make the results better [1].
8. **Recognize that net-centric operations are not a panacea.** Increased asset and data visibility may encourage

micromanagement. Recent experience in Afghanistan and Iraq has shown that:

> …another consequence of our expanded global connectivity was that *reach-back*, a desirable capability when used with discrimination, metamorphosed into *reach-forward* as rear headquarters sought information… and then used that information to try to influence events from the rear. [5]

It is ironic that net-centric operations enables both *reach back* (providing increased information for local leaders to make decisions) and *reach forward* (providing rear headquarters with additional information and an increased temptation to micromanage). There must be a balance reached between centralized planning and local execution.

9. **Be patient.** The DoD has been actively working on net-centric warfare for several years, but as John G. Grimes, DoD-CIO, recently noted:

> Unlike designing a tank or launching a satellite, our transformation to net-centric operations is traversing new ground. We stand at the brink of an era when networked capabilities will increase efficiency, enhance mission success, save lives and potentially reduce force structure… [2]

Conclusion

The DoD is in the process of transforming to net-centric operations. Net-centric railroading could be the key to making railroads safer, reducing delays and costs, raising effective capacity, increasing reliability, improving customer satisfaction, improving energy utilization, reducing emissions, increasing security, and making railroads more economically viable. At the same time, these efforts should provide numerous opportunities for sharing hardware, software, and experiences.

Grimes recently summarized:

> Net-enabled operations, while clearly complex, can actually be described quite simply. It is all about ensuring timely and accurate information gets where it's needed, when it's needed and to those who need it most. [2]

This is equally true for the DoD, the DoT, the railroad industry, other modes of

transportation, and other government agencies. Reasonable sharing of plans, research, experience, and lessons learned regarding net-centric operations should be in everyone's best interest.◆

References

1. Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. DoD C4ISR. Washington: Cooperative Research Program (CCRP) 1999.
2. Grimes, John G. "A Chat with John G. Grimes, New Defense CIO." Defense Systems Jan./Feb. (2006): 14+.
3. Weick, Karl E., and Kathleen M. Sutcliffe. Managing the Unexpected. San Francisco: Jossey-Bass, 2001.
4. Atkinson, Rick. "The Long, Blinding Road to War: Unexpected Challenges Tested Petraeus in Iraq." The Washington Post 7 Mar. 2004: A1 <www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A36 843-2004Mar6&notFound=true>.
5. Lambeth, Benjamin S. "The Downside of Network-Centric Warfare." Aviation Week and Space Technology 11 Feb. 2006.

Notes

1. Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD, 23 Apr. 1997.
2. Available online at <www.bts.gov/publications/the_changing_face_of_transportation/>.
3. Available online at <www.fra.dot.gov/us/content/225>.
4. Available online at <www.tea.army.mil/DODProg/RND/default.htm>.
5. Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." Proc. of U.S. Naval Institute, Jan. 1998.
6. The NTSB's most wanted list is found at the NTSB Web site <www.ntsb.gov/Recs/mostwanted/rail_issues.htm>.

About the Authors

COL Kenneth L. Alford, Ph.D., is a professor and department chair at the Industrial College of the Armed Forces at the National Defense University in Washington, DC. He has served 26 years in the Army as a personnel, automation, and acquisition officer in a wide variety of duty assignments, including his previous position as an Associate Professor in the Department of Electrical Engineering and Computer Science at the United States Military Academy, West Point, NY. He has a doctorate in computer science from George Mason University, masters degrees from the University of Illinois at Urbana-Champaign and the University of Southern California; and a bachelor's degree from Brigham Young University.

Industrial College of the Armed Forces
National Defense University
Washington, D.C. 20319
Phone: (202) 675-4408
Fax: (202) 685-4175
E-mail: alfordk@ndu.edu

Steven R. Ditmeyer joined the Industrial College of the Armed Forces as the DoT Faculty Chair in 2003. He served his Army active duty tour with the Office of the Special Assistant for Strategic Mobility in the Organization of the Joint Chiefs of Staff, and in the Army Reserve he served with the Military Traffic Management and Terminal Service and Head Quarters, 3rd Transportation Brigade (Railway). Ditmeyer's civilian career has been in a number of transportation-related positions in both the public and private sectors. He received a bachelor's degree in industrial management from the Massachusetts Institute of Technology, a masters degree in economics, and a Certificate in Transportation from Yale University where he was a Strathcona Fellow in Transportation.

Industrial College of the Armed Forces
National Defense University
Washington, D.C. 20319
Phone: (202) 685-4375
Fax: (202) 685-4175
E-mail: ditmeyers@ndu.edu

Profiles of Level 5 CMMI Organizations

Donald J. Reifer
Reifer Consultants, Inc.

Many firms that have achieved Level 5 using the Software Engineering Institute's Capability Maturity Model® Integration (CMMI®) have taken a different tact in justifying their process improvement initiative's budget. This article summarizes the profiles of high maturity organizations and explains how they go about justifying their budgets. The article also provides insight into the differing tactics that these firms use to win the battle of the budget and the reasons for them.

During the past two decades, a number of professionals in the software community have argued for investing in process improvement [1, 2]. Those following the mantra of embracing frameworks like the Software Engineering Institute's CMM [3] and CMMI [4] have touted the benefits of process improvement and argued that the costs are fully justified [5, 6]. While there are some definitive works that portray the cost/benefits [7, 8], little has been done to study the return on investment (ROI) of high maturity organizations that have reached Level 5. Many practitioners within the industry that we have talked with wonder what happens when high maturity organizations move into the maintenance mode at Level 5. Managers wonder what the costs/benefits are and what others' experiences have entailed. Process groups want to know how to justify the costs of sustaining a process improvement program in a maintenance mode. In fact, everyone we spoke with wanted to be able to set realistic expectations for their continuous improvement efforts. However, the only data that seemed available to them referred to the benefits associated with reaching higher CMM [9] and/or CMMI maturity levels [10]. Based on our research, we can conclude that little data exists that firms can use to justify maintaining their process improvement programs at either CMM or CMMI Level 5. In addition, those that report about their performance typically mix CMM and CMMI data in their analysis (see CMMI performance results about Level 5 firms on the Software Engineering Institute [SEI] Web site at <www.sei.cmu.edu>).

The Study

Early last year, we embarked on a study to develop answers to these questions. Three process groups from different organizations sponsored an effort aimed at using historical data to justify their process improvement maintenance budgets at CMMI Level 5. To begin, we contacted those Level 5 firms within the United States listed on the SEI's Web site with which we had a relationship and asked them for permission to use their data without attribution to develop our results. For the past 20 years, we have been working with organizations like those that sponsored our effort to develop cost, productivity, and quality benchmarks [11]. For the most part, the 11 firms and 19 organizations that agreed to supply us during the past 18 months with data shared the profile summarized in Table 1. As the table illustrates, the organizations surveyed were large, distributed, hierarchical, and primarily working within either the aerospace or telecommunications industries. Their primary motivation for being Level 5 was both to be competitive (e.g., most of their competitors perceived as Level 5 are using CMMI), and able to deliver what they promised to their customers on time and within budget (i.e., improve their ability to predict and control their system/software engineering activities).

Foreign firms were specifically excluded from our analysis because all those involved felt that they would bias the results. To confirm this tendency, we analyzed the resulting databases with and without foreign contributions and discovered that it was a better fit with the foreign data eliminated because the underlying databases were more homogeneous. For example, data on Level 5 firms collected from India was primarily from United States subsidiaries developing software for commercial applications as opposed to aerospace applications. These organizations were mid-sized (averaged about 250 to 500 engineers), and minimal system and hardware engineering was performed. Based on these facts, we agreed not to include foreign data. However, we may decide differently in the future as we populate our databases.

Table 1: *Profile of United States Level 5 Organizations Used in Analysis*

Characteristic	Explanation
Industry	Aerospace
Major Products	Aircraft, missiles, satellites, spacecraft, tactical systems, weapons systems, etc.
Management Organization	Hierarchical with many layers of management. Matrix approach used for the most part with program management separate from contracts and engineering. Engineering budgets cover Research and Development and investments to develop skills (training) and processes.
Engineering Workforce Size	Average size of performing organizations with more than 1,000 engineers/location.
Number of Locations	Average greater than five with workforce distributed either based on product lines or legacy firms that they had acquired.
Process Framework Embraced	CMM and CMMI – all were Level 5 and all had transitioned to the use of the CMMI (some were being re-evaluated for Level 5).
Process Organization	Process group with a staff of approximately five, and a budget averaging about $2 million per year (besides funding staff, they provided budgets for training, tools, the Process Asset Library, etc.).
Years Pursuing Process Improvement Initiatives	More than 10 years on average working to raise the level of the organization to Level 5 first using the CMM and now the CMMI.
Investment Climate	Process improvement viewed as a customer requirement; emphasis on minimizing overhead expenses.

Determining the Costs/Benefits

We next analyzed our databases to determine the costs needed to maintain and sustain a process improvement program and the benefits that resulted at Level 5. Costs and benefits were collected by scenario as shown in Tables 2 and 3 and briefly defined as the following:

- **Optimization and Maintenance.** Rather than focusing on achieving higher maturity levels, the process staff focuses on maintaining processes and perfecting their use. They modify processes, optimize them and increase their holdings in their Process Asset Libraries. They focus on making processes work better by incorporating feedback based on operational use.
- **Focus on Finding Defects Out-of-Phase.** The process staff reinvents itself and places emphasis on embracing six sigma techniques to prevent defects from occurring earlier in the life cycle. They capitalize on their statistical process control experience to reduce escapes (defects escaping from one phase to the next; e.g., a requirements defect that escaped and was not found until the design phase).

For completeness, we have included the cost/benefit data previously collected as part of another one of our ongoing efforts relative to starting up a process program and reaching higher maturity levels as shown in Tables 2 and 3 [12]. These two additional process improvement scenarios are briefly defined as the following:

- **Starting Up.** Initiating a process improvement program, selling the concept, staffing the process team, writing the processes, and providing the training and project support needed to fan out throughout the organization.
- **Reaching for Higher Maturity Levels.** Moving from one level to the next in process maturity includes the effort to satisfy the framework requirements and survive and recover from a CMMI assessment [13]. As Table 2 shows, reaching the next level in process maturity involves a great deal of effort and takes between 15 and 21 months to achieve.

Level 5 activities by design are aimed at optimizing existing processes, not developing, introducing or institutionalizing new ones. Statistical process control techniques are used to determine which processes are working well and which are not. Those maintaining processes use this information to focus their resources on making processes work better through training, mentoring, and improving organizational support.

The following important points amplify some of the points raised within Tables 2 and 3:

- Process improvement budgets for starting up a program and focusing on reaching the next level of process maturity are two to three times higher than those for optimization and maintenance. This makes sense based on

Scenario	Range of Cost/Time ($ expended/months to complete)+		
	Small	**Medium**	**Large**
Starting Up	$1 to 1.5M/ 18 to 20 months	$1.5 to 2.5M/ 18 to 22 months	$2.5 to 3M/ 20 to 24 months
Reaching the Next Level in Process Maturity	$0.75 to 1M/ 12 to 16 months	$1 to 1.5M/ 15 to 18 months	$1.5 to 2M/ 18 to 21 months
Optimization and Maintenance	$0.35 to 0.5M/ 12 months++	$0.5 to 0.75M/ 12 months++	$0.75 to 1M/ 12 months++
Out-of-Phase Defect Focus	$0.5 to 0.78M/ 12 months++	$0.78 to 1.0/ 12 months++	$1.0 to $1.3M/ 12 months++

+ Costs incurred are those for the process improvement program. Burdened cost per person-month average $20K (2005 year $. Staff involved in process improvement programs in large firms tends to be very senior and therefore very expensive [i.e., groups are typically staffed with opinion leaders who have the respect of the workers based on their accomplishments with 20+ years of experience]).

* Typical staff assigned to process group between four and six equivalent heads; three work process development, and three provide project support either as part of the process group or within project organization.

++Budgeted/reported on an annual basis.

Table 2: *Range of Costs/Time by Scenario for Military Systems by Organization Size*

Table 3: *Range of Benefits for Military Systems by Scenario*

Benefit Category	Benefit Range/Time ($ saved/months to realize)+			
	Starting Up	**Reaching the Next Level**	**Optimization and Maintenance**	**Out-of-Phase Defect Focus**
Cost Avoidance	2 to 12% savings/ 18 to 20 months*	3 to 16% savings/ 16 to 18 months	Flat	Finding escapes results in 6 to 8% savings/ annually
Productivity Gains	5 to 10% annually*	8 to 18% annually	Flat	1 to 3% annually
Faster Time-to-Market	Not applicable during startup	Improved ability to predict/meet schedule	Improved ability to predict/meet schedule	Improved ability to predict/meet schedule
Quality Improvement	Not enough data	8 to 18% fewer errors/post release	12 to 26% fewer errors/post release	18 to 30% fewer escapes
Estimated ROI	15 to 51%/ 18 to 20 months	18 to 103%/ 15 to 18 months	12 to 36%/ annually	24 to 138%/ annually
Minimum Time (to achieve ROI)	18 months	15 months	Performed on an annual basis	Performed on an annual basis
Other benefits:				
■ Improved customer satisfaction	Fewer customer complaints	Increased customer praise	Continued customer praise	Customer views you as best in class
■ Improved competitive positioning ■ Other	Perceived competitive gaps closed	Perceived competitive gaps closed	Continued commitment to process maintained	Perceived competitive advantage

+ Benefits computed for the entire engineering organization at large. Burdened cost per person-month is less than that for the process improvement effort averaging $15K (2005 year $) (**Note** – staff involved in the development organization are typically less qualified than those involved in the process group).

* Many organizations that start up a process program make the mistake of promising results in the first year. Because of learning curves and start-up problems, positive results do not accrue until the second year when the appraisal is conducted and confirmation is made that they have realized their goals.

++ Budgeted/reported on an annual basis.

the relative efforts involved. However, just like many software development efforts, many process groups claim premature victory when they get appraised at Level 5. While most organizations embrace the processes, some object to them. In addition, new projects need considerable start-up support that the process group is expected to provide. Finally, because benefits are not as visible, there is pressure from upper management to dissolve the process group and use the overhead money that funds them for other purposes.

• Things seem to improve when Six Sigma techniques are coupled with process optimization and maintenance activities. Emphasis is placed on business performance rather than process goals as evidence is gathered to justify continuance and possible expansion of the program [14]. Budgets are justified because benefits are made visible and overhead funds are not diverted to other activities.

• Focusing on defects pays dividends as errors are found sooner and their root causes are systematically identified and addressed. Defects are caught in-phase (e.g., requirements errors are found and fixed during the requirements phase) and, as such, are easier, cheaper and simpler to remove. Emphasis is placed on defect prevention as well as reduction as processes are refined and optimized. New methods and tools like those for Six Sigma are acquired to automate these processes and make defect prevention part of the way work is done by performing organizations [15]. Designs are made more robust because root causes of persistent defects are eliminated, customer satisfaction is improved, and the organization's reputation for quality is enhanced.

• The ROI picture changes as the cost/benefits of the program are compiled. Instead of portraying the status quo, defect prevention is emphasized.

When the ROI for process improvement is computed using numbers like those provided in Table 3, the cumulative returns along with the list of other compelling factors can easily be used to convince executive management that their investments in process improvement make both good financial and technical sense. As an aside, we have found the use of the balanced scorecard to be a good way to present this data to executives in a holistic manner [16].

Looking at an example, one of our sponsors brought us in to assist them in preparing a briefing to senior management about the ROI of process improvement. When we delved further, we found that the briefing was aimed at convincing senior management not to eliminate the process group that had led their efforts during the past seven years in achieving a Level 5 rating. As expected, they had captured a great deal of cost, productivity and quality data as part of their metrics and statistical process control efforts. Unfortunately, the data validated the trends summarized in Tables 2 and 3; i.e., cost and productivity gains at Level 5 were flat and defect removal data alone did not justify the group's expenses (i.e., included the personnel assigned to the group along with training and facilitation expenses associated with fanning the process out to the projects). This group of five had been at Level 5 for four years, and was reappraised Level 5 CMMI last year. Senior management was not impressed by the business case presented to them during the last quarter and as a result were toying with the idea of dissolving the group and spending the money elsewhere (where ROI of the investment seemed better).

When we analyzed the organization's benefits data, we saw their focus was being placed on reducing the variation in organizational performance across projects – a function of process tailoring and utilization. The statistical data was very valuable

in this regard because it showed which processes were working well and which were not. We pointed out that there were high yield processes that had not been identified by the CMMI that still needed work; e.g., notably COTS management and software licensing. For example, we commented that we had saved one of our clients several million dollars annually by helping them put an enterprise licensing scheme in place for their software development tools [17]. We also suggested that more emphasis on preventing defects from escaping from one phase to another (escapes) could result in substantial increases in their yields. When we briefed these opportunities to the senior management, they became excited and tasked their process group to pursue additional process development, rollout, and defect prevention as part of their three-year plan. More importantly, budgets were approved as the process group took on this new mission.

Making the Business Case in High Maturity Firms

For large organizations like those involved in our survey, it is relatively easy to justify starting up or pursuing a process improvement initiative. However, it is more difficult to develop a business case when pursuing Level 5 optimization and maintenance activities [18]. Because cost and productivity gains are flat, firms often pare their process efforts down considerably at this stage. Those that reinvent themselves and place emphasis on Six Sigma techniques are the exception. For these organizations, the benefits derived by reducing defects across life-cycle stages (i.e., the number of escapes) seem sufficient to justify continuation of their efforts. However, such economies of scale may not be available for smaller organizations. As a result, building a business case under such circumstances becomes much more difficult.

Firms surveyed were somewhat surprised when we concluded that cost avoidance and productivity gains held steady once they reached Level 5. The easiest way to explain to them what was happening with cost and productivity was to make the following analogy. Say you go on a diet and lose 10 pounds during the first month. If you wanted to lose an additional 100 pounds at this rate, it would take you 10 months at 10 pounds per month. However, while losing weight is easy at first, it becomes more difficult as the pounds come off. Many times during your diet your weight stabilizes and it becomes extremely difficult to shed even a few

Table 4: *Range of Cost to Find and Fix Defects In-Phase and Out-of-Phase*

Injected / Found	Range of Cost to Find and Fix Defects In-Phase and Out-of-Phase+			
	Inception	**Elaboration**	**Construction**	**Transition**
Inception	$25 to $100/defect			
Elaboration	$100 to $500/defect	$50 to $250/defect		
Construction	$500 to $1K/defect	$250 to $1.5K/defect	$75 to $500/defect	
Transition	$8K to $10K/defect	$1.5K to $5K/defect	$500 to $3K/defect	Not enough data

+ Defect costs computed for the entire engineering organization at large. Burdened cost per person-month again averages $15K (2005 year $).

additional pounds. Then, when you reach your weight loss goal, you have to go on a maintenance diet or else you will quickly gain the weight back. Cost avoidance and productivity gains are similar to weight loss. They occur quickly at first as you introduce processes and discipline. Once the processes are institutionalized, productivity gains and cost avoidance then stabilize and happen less quickly. As a result, when processes reach a steady state (e.g., at Level 5), cost avoidance and productivity gains become minimal. Similar to when you finish your diet, this stability should be expected.

For high maturity organizations at CMM and CMMI Level 5, justification for continuing process improvement work is handled differently. Based on the data we have collected and the experiences of firms polled, we can make the following observations:

- The emphasis of process improvement initiatives rightfully shifts from moving from one level of process maturity to the next to maintenance and optimization of the program.
- Organizations learn to use statistical process control information to optimize their use of resources. For example, projects shift personnel from one process to another when their control charts indicate that they are being successful with their practices (e.g., from inspections to test when inspections are working well).
- As a consequence of shifts in emphasis, cost avoidance and productivity gains tend to remain relatively flat for Level 5 organizations. The reason for this seems to be that high maturity organizations tend to focus on optimizing the use of existing processes instead of placing emphasis on reaching the next level of process maturity. Without the push to move ahead, the organization loses its drive and momentum.
- Cost avoidances tend to be negligible when organizations reach either SW-CMM or CMMI Level 5 because typically their resources are scaled back to pursue maintenance and optimization rather than the active pursuit of moving from one maturity level to the next.
- Defect rates and densities during both development and post-release phases of the life cycle tend to stabilize as organizational processes become institutionalized.
- In many organizations, process groups are disbanded. The process improvement charter is not dropped. Instead, it is picked up by other support groups (qual-

ity assurance, etc.) or initiatives (knowledge management, Six Sigma, etc.).

Domain of Applicability

The findings and observations shared in this article tend to be applicable to large projects where economies of scale make justification of investments in process improvement typically easy. This makes sense because most U.S. organizations that have been appraised Level 5 in the current Software Engineering Institute (SEI) process maturity database [19] are military/government agencies or their con-

"Successful process improvement groups reinvent themselves in high maturity organizations at CMMI Level 5. To justify their existence, they take on new charters and new initiatives to move their organizations forward and preserve their budgets."

tractors (72 percent or 230 of those 321 reporting results). For the most part, these organizations share the organizational profile provided in Table 1. Even with this as the case, it is important to note that our conclusions may not be shared by either small firms or with foreign enterprises that make up 60 percent of the SEI appraisal database.

Conclusion

Successful process improvement groups reinvent themselves in high maturity organizations at CMMI Level 5. To justify their existence, they take on new charters and new initiatives to move their organizations forward and preserve their budgets. Those that we have observed to be successful defend their budgets based on reducing escapes, developing processes aligned with improving business functions (licensing, COTS management, etc.) and/or by achieving knowledge transfer goals. They embrace techniques like Six Sigma and

lean manufacturing, using them to focus on improving quality in addition to productivity, time-to-market or cost. Budget justification is relatively easy because, as noted in Table 4, they reduce escapes (e. g., finding and fixing defects out-of-phase) whose costs can be as great as 400 to one in the worst case.

The message from our analysis for high maturity organizations is loud and clear: Once they have institutionalized their processes, they should refocus their efforts on goals aligned with improving the business (improved product quality, etc.). As part of this reorientation, they should restructure their metrics program to capture additional data that can be used to measure the value of their business propositions. When implementing statistical process control at Level 5, they should embrace Six Sigma concepts to reduce defects in both their processes and products. They should focus on preventing defects by finding and fixing them by using techniques like orthogonal defect classification [20]. We believe that embracing Six Sigma and black belt concepts for both process and product improvement activities would be synergistic. Finally, Level 5 organizations should consider using the cost/benefits associated with finding and fixing defects as a means to justify their investments in process improvement. Use of such an approach makes it relatively easy to build the business case for process groups to pursue these revamped rather than new courses of action.◆

References

1. Diaz, M., and J. King. "How CMM Impacts Quality, Productivity, Rework, and the Bottom Line." CROSSTALK Mar. 2002 <www.stsc.hill.af.mil/cross talk/2002/03>.
2. Pitterman, B. "Telecordia Technologies: The Journey to High Maturity." IEEE Software 17.4 (2000): 89-96.
3. Paulk, M.C., C.V. Weber, B. Curtis, and M.B. Chrissis. The Capability Maturity Model: Guidelines for Improving the Software Process. Addison-Wesley, 1995.
4. Chrissis, M.B., M. Konrad, and S.

Shrum. <u>CMMI: Guidelines for Process Integration and Product Improvement</u>. Addison-Wesley, 2003.

5. Yamamura, G., and G.B. Wigle. "SEI CMM Level 5: For the Right Reasons." CROSSTALK Aug. 1997 <www.stsc.hill.af.mil/crosstalk/1997/08>.

6. Walden, D. "A Business Case for CMMI-Based Process Improvement." Proc. of PSM Conference, July 2002.

7. Scott, W. "The Business Benefits of CMMI at NCR Self-Service." London: European Software Engineering Process Group, June 2004.

8. Freed, D. "CMMI Level 5: Return on Investment for Raytheon." CMMI Technology Conference, Denver, CO; Nov. 2004.

9. Clark, B. "The Effects of Process Maturity on Software Development Effort." University of Southern California Report No. USC-CSE-97-510. Aug. 1997.

10. Goldenson, D.R., D.L. Gibson, and R. W. Ferguson. "Why Make the Switch? Evidence About the Benefits of CMMI." Software Engineering Process Group, 2004.

11. Reifer, D.J. "Software Cost, Quality, and Productivity Benchmarks," <u>The DoD Software Tech News</u> 7.2 (2004): 3-8, 17-19.

12. Reifer, D.J. "Making the Case For and Against Process Improvement." Systems and Software Consortium Report No. SSCI-2005030-MC. Dec. 2005.

13. Ahern, D.M., et al. <u>CMMI SCAMPI Distilled</u>. Addison-Wesley, 2005.

14. Hefner, Rick. "Accelerating CMMI Adoption Using Six Sigma: Northrop Grumman Case Study." CMMI Technology Conference and User Group 15-18 Nov. 2004.

15. Mullen, R. "Orthogonal Defect Classification at Cisco Systems." Proc. of Industry Day, The International Symposium on Software Reliability Engineering and the International Conference on Software Maintenance, San Jose, CA: Oct. 2000.

16. Grembergen, W. Van. "The Balanced Scorecard and IT Governance." Information Systems Control Journal Vol. 2 (2000).

17. Reifer, D.J. "Software Licensing: A Target of Opportunity for Process Improvement." Proc. of the Acquisition Management Conference, Defense Systems Management College, June 1999.

18. Reifer, D.J. "Making the Software Business Case: Improvement by the Numbers." Addison-Wesley, 2002.

19. SEI. "Process Maturity Profile: CMMI v1.1 SCAMPI v1.1 Class A Appraisal Results." SEI. Sept., 2005.

20. Chillarage, R., et al. "Orthogonal Defect Classification – A Concept for In-Process Measurements." <u>IEEE Transactions on Software Engineering</u> 18.11 (Nov. 1992): 943-956.

About the Author

Donald J. Reifer is president of Reifer Consultants, Inc., where he advises executives in Fortune 500 firms on software investment and improvement strategies. He has more than 35 years experience in software engineering and management for industry and government. From 1993 to 1995, Reifer managed the Department of Defense Software Initiatives Office under an Intergovernmental Personnel Act assignment with the Defense Information Systems Agency. Reifer served as deputy program manager for TRW's Global Positioning Satellite efforts. While with the Aerospace Corporation, he managed all software efforts related to the space transportation system (space shuttle). He has a bachelor's degree in electrical engineering from New Jersey Institute of Technology and a master's degree in operations research from the University of Southern California.

Reifer Consultants, Inc.
P.O. Box 4046
Torrance, CA 90510-4046
Phone: (310) 530-4493
Fax: (310) 530-4297
E-mail: d.reifer@ieee.org

LETTER TO THE EDITOR

Dear CROSSTALK Editor,

Allow me to comment on the number one lesson learned that was in David Webb's October CROSSTALK article *All We Need to Know About Software Project Management, We Can Learn From Star Trek*.

I discovered early on, long before *Star Trek* ever aired episode one, that whilst I could make good estimates for how long it would take me to do a given software task, management always cut the estimate in half. Possibly because they thought everyone always overestimated, and certainly in part because they had overpromised the customer. There were certainly many people who did not know how to estimate and made wild guesses that helped reinforce management's need to question all estimates. Consequently, I started doubling my estimates only to discover that the time I lost waiting for others, attending meetings, doing administrivia, guarding turf, politicking for my manager, context switch inefficiency, yada yada, still took as long as the actual work.

Unfortunately, management thinks this unproductive work/time is *free* and takes no calendar time. As a result, I have made it a policy to always multiply my estimates by (at least) four. This lets management do their obligatory cut, and provides time for the non-productive tasks that always occur.

If management were truly CMM/CMMI conformant, they would allow adequate resources and encourage accurate allocation of same. In spite of all the CMM/CMMI hoopla and appraisals, far too many organizations are truly conformant only to the extent of having a certificate on the wall. So, until the millennium is upon us, I will continue to teach my students to multiply their estimates by four before committing to a task. I also warn them not to let others impose their estimates on us because the estimates will be both overly optimistic and will omit the overhead and time wasters that are required.

If my strategem made it into *Star Trek III*, then apparently others have had the same experiences and came up with similar solutions.

As to miracles, maybe in *Star Trek*; but in my real-world experience, when the occasional miracle is performed management uses it as proof that their overly optimistic estimating is right and the workers are all lazy slackers who pad everything.

– Dr. William Adams, PE
williamadams@ieee.org

Enterprise Software Initiative (ESI)

www.esi.mil

The ESI aims to lead in the establishment and management of enterprise commercial off-the-shelf information technology agreements, assets, and policies for the purpose of lowering total cost of ownership across the Department of Defense (DoD), Coast Guard, and intelligence communities.

The Internet Governance Project (IGP)

www.internetgovernance.org

The IGP is a consortium of academics with scholarly and practical expertise in international governance, Internet policy, and information and communication technology. IGP conducts research on and publishes analysis of global Internet governance. The work is intended to contribute to policy discussions in the Internet Governance Forum, Internet Corporation for Assigned Names and Numbers, World Intellectual Property Organization and related debates at the global, international, regional and national levels.

The goal of the IGP is to:
•   Inform and shape Internet public policy choices by providing independent analysis and timely recommendations.
•   Identify and analyze new possibilities for improving global governance institutions.
•   Develop policy positions guided by the values of globalism, democratic governance and individual rights.

The IGP is being supported through a two-year opportunity grant from the Ford Foundation.

The United Nations Information and Communication Technologies Task Force

www.unicttf.org

In March 2001, the Economic and Social Council requested the Secretary-General to establish an Information and Communication Technologies (ICT) Task Force. This initiative is intended to lend a truly global dimension to the multitude of efforts to bridge the global digital divide, foster digital opportunity and thus firmly put ICT at the service of development for all. The ICT Task Force is supported by the Heads of State and Government of all United Nations Member States who endorsed the Economic and Social Council Ministerial Declaration at the Millennium Summit in September 2000.

The objective of the Task Force is to provide overall leadership to the United Nations role in helping to formulate strategies for the development of information and communication technologies and putting those technologies at the service of development and, on the basis of consultations with all stakeholders and Member States, forging a strategic partnership between the United Nations system, private industry and financing trusts and foundations, donors, program countries and other relevant stakeholders in accordance with relevant United Nations resolutions.

National Science and Technology Council (NSTC)

www.ostp.gov/nstc

NSTC was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials. A primary objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals. The work of the NSTC is organized under four primary committees: Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees subcommittees and working groups focused on different aspects of science and technology and working to coordinate across the federal government.

Networking and Information Technology Research and Development (NITRD)

www.nitrd.gov

The National Coordination Office (NCO) for NITRD supports the planning, budget, and assessment activities for the Federal government's NITRD Program. The NCO reports to the White House Office of Science and Technology Policy and the National Science and Technology Council (NSTC). The NCO supports the participating Federal agencies through the NSTC's Subcommittee on NITRD, Interagency Working Group on High End Computing, Interagency Working Group on Cyber Security and Information Assurance, and five Coordinating Groups to prepare and implement the NITRD budget crosscut, totaling over $3 billion in fiscal year 2007. Federal information technology research, which launched and fueled the digital revolution, continues to drive innovation in scientific research, national security, communication, and commerce to sustain U.S. technological leadership. The NITRD agencies' collaborative efforts increase the overall effectiveness and productivity of Federal networking and information technology Research and Development (R&D) investments, leveraging strengths, avoiding duplication, and increasing interoperability of R&D products.

Sticky Minds

www.stickyminds.com

StickyMinds.com, a comprehensive online resource for helping produce better software, offers an unrivaled scope of original articles from industry experts, technical papers, industry news, a searchable tools and books guide, discussion forums, and more. StickyMinds.com is the online companion to *Better Software* magazine. StickyMinds.com is the Web's first and most popular interactive community exclusively engaged in improving software quality throughout the software development life cycle. Membership is free.

One If By LAN,
Two If By C

I am a process-oriented guy. While I am on the safe side of Obsessive-Compulsive Disorder Guy, I'm not too far off. I have an internalized ritual for many facets of my life. My computing, of course, is extremely organized. I perform monthly backup of my computer hard drive (because I'm *experienced* – and have worked on far too many computer systems that crashed with extreme regularity). I perform weekly backup of critical data. I manage to synchronize an office desktop, a personal laptop, a home desktop, and a second laptop that my wife and daughter use but is always hot-swappable for my laptop in case of an emergency.

So when my company recently offered to replace my functional but aging laptop with a top-of-the-line desktop, who was I to refuse dual 21-inch LCD monitors? With everything I have backed up, how hard could it be?

The *Transfer File* and *Settings* wizard was outdated on the older machine. Once updated, it complained about going from a 32-bit laptop to a 64-bit desktop. I use Firefox for now (gotta love that Tabbed Browsing – hurry up Internet Explorer 7.0!) and there is no simple way to transfer saved passwords. Have you looked at how many extensions you have in your browser? Note that they *do not* transfer.

Need I mention that there is a slight chance that I use a *few* third-party applications? Wonder where the install disks are? Did I bother to save the registration code from when I downloaded most of them from the Internet? Do they work with the new drivers? What are the hidden settings of most of these third-party applications?

Oh my gosh – I must have about 100+ fonts installed on the laptop. Do I transfer them all (thus slowing down the new system)? Or do I weed out those I'm sure I'll never use? (And where in the world did I EVER get a font named Cappucino?) Do you have ANY idea how many updates to XP and Office are needed with a new system? Why does every application update seem to require a separate reboot?

The old laptop and single monitor were small in terms of real estate. The new desktop is too big for the desktop and needs to sit on the floor. How come the video cables are ALWAYS (HURCULANUM – what kind of name is that for a font?) too short. Hey, with eight USB ports, I can hook up all of the assorted hard drives that I have accumulated. Why are there only six outlets on the surge suppressor?

Been there? You know, I haven't migrated from one machine to another in more than three years. Used to be that all of my *stuff* used to fit on a single CD. Now, my *My Documents* folder alone requires four dual-layer DVDs. Just like people accumulate stuff in their house, you accumulate stuff in your *My Documents* directory.

It took three days, but I'm finally up and running again. I seem to have accounted for all of the items mentioned above, and even managed to reconnect the personal folders under Outlook.

Could I do this over again with less bother? Oh yeah. In fact, I even managed to create a folder on my hard drive called *Application for Reinstall*. I also cleared out a desk drawer and put all of the CDs and DVDs in one place just in case there is a next time. And, of course, I made a commitment to continually update both the folder and desk drawer over the next three years. Unless I forget. Or get too busy.

This is why you need a process in your professional life. Processes let you learn from the mistakes or tribulations of others (or, if you're REALLY good, you can actually learn from yourself!). In days gone by, I have sung the praises of CMM and CMMI. I have taught the PSP℠ (Personal Software Process℠) to any developer and engineer who would sit still. And, over the years, I have come to understand and appreciate Agile methodologies.

It's all about sizing. I once consulted for a military organization that was CMM Level 4, well on their way to CMM Level 5. They were so good that a fellow organization decided to adopt their practices. Unfortunately, the first organization had more than 100 personnel while the second had around 20. While the first organization eventually soared on to greatness, the second organization spent SO (Jester font) much time working on the process, that they never produced anything.

Processes are like shoes. They're personal. What fits one might not fit another. Some folks need industrial-strength, steel-toe, slip-resistant, oil-and-water-resistant boots. Others can live with $5 flip-flops. If you try to create a shoe (or a process) that fits EVERYBODY (Marker Felt font), then it fits nobody. It's like a caffeine-free diet soda: It doesn't really provide anything (and can give you gas).

Need a process? It's like shopping for shoes. Need Manolo Blahnik shoes (hey, I used to watch *Sex in the City*)? Or will a workable and affordable pair from Payless work? Need heavy-strength CMMI? Will Agile work for you? It depends: Are you building a mission-critical real-time distributed application? Or a relatively simple Web application?

It's all about fit.

— **David A. Cook, Ph.D.**
Senior Research Scientist and
Principle Member of the Technical Staff
The AEgis Technologies Group, Inc.
dcook@aegistg.com (Papyrus font)

Perpetua Poor Richard **Haettenschweiler** FELIX TITLING

Colonna MT **GOUDY STOUT** Bauhaus 93

Bodoni MT Condensed **Eras Bold ITC** *Forte*

℠ Personal Software Process and PSP are service marks of Carnegie Mellon University.

CrossTalk / 517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

PRSRT STD
U.S. POSTAGE PAID
Albuquerque, NM
Permit 737